(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－539487
（P2002－539487A）
(43)公表日　平成14年11月19日(2002.11.19)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		５Ｂ０５７
Ｇ０６Ｔ　1/00	５００	Ｇ０６Ｔ　1/00	５００Ｂ	５Ｃ０６３
Ｇ１０Ｋ　15/02		Ｇ１０Ｋ　15/02		５Ｃ０７６
Ｇ１０Ｌ　11/00		Ｈ０４Ｎ　1/387		５Ｊ１０４
Ｈ０４Ｎ　1/387		Ｇ１０Ｌ　9/00	Ｅ	

審査請求　未請求　予備審査請求　有　（全104頁）　最終頁に続く

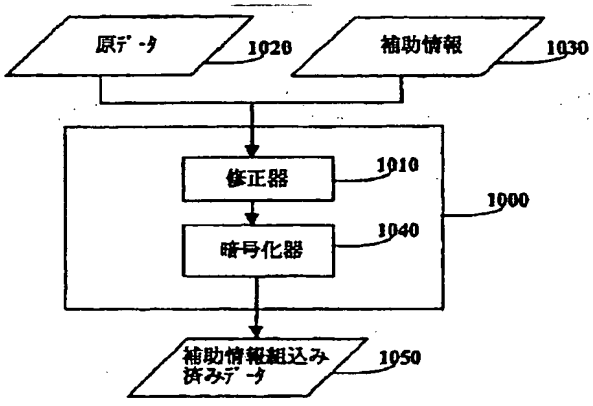
(21)出願番号　特願2000－604566(P2000－604566)
(86)(22)出願日　平成12年３月10日(2000.3.10)
(85)翻訳文提出日　平成13年９月10日(2001.9.10)
(86)国際出願番号　ＰＣＴ／ＵＳ００／０６２９６
(87)国際公開番号　ＷＯ００／５４４５３
(87)国際公開日　平成12年９月14日(2000.9.14)
(31)優先権主張番号　６０／１２３，５８１
(32)優先日　平成11年３月10日(1999.3.10)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　６０／１２３，５８７
(32)優先日　平成11年３月10日(1999.3.10)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ディジマーク　コーポレイション
アメリカ合衆国　オレゴン　97062，テュアラティン，エスダブリュー　72エヌディー　アベニュー　19801　スイート　100
(71)出願人　アコースティック　インフォメーション　プロセシング　ラブ　エルエルシー
アメリカ合衆国　ワシントン州　98648　スティーヴンソン　エヌイー　セダール　ストリート　110
(74)代理人　弁理士　杉村　興作　（外１名）

最終頁に続く

(54)【発明の名称】　信号処理方法及び装置

(57)【要約】
電子的コンテンツ（例えばオーディオ、ビデオ、静止画像、等）(1020)に補助データ(1030)を、簡単な演算で補助データが目立たないような方法(1010)で通信秘匿的に埋め込む技法について詳述する。埋め込みデータは著作権または他の所有権情報を載せることができ、あるいは装置制御目的に用いることができる。補助データを除去することに対しては、コンテンツを、補助データが存在することへのキーに用いることを含めた多数の対策が考案されている。例えばメディアの特性に従って埋め込みデータを修正することによって、メディアに応じた埋め込みデータを作成することができる。暗号化法を採用(1040)して有利にすることもできる。前にアクセスしたコンテンツからＩＤをたどって使用規則を施行するように、再生装置を製品化することができる。一部の実施例は多数の透かしを採用して有利にしたものであり、例えば、配布の前に強固な透かしを符号化してコンテンツが保護されていることを示し、そして第２の透かしを再生装置によって符号化して、コンテンツをこの装置に一意的にリンクする。一部の応用では、所定の情報（例えば



【特許請求の範囲】

【請求項１】　複数ビットの補助データをコンテンツ内に通信秘匿的に符号化する方法であり、前記コンテンツが、複数サンプルから構成されるオーディオ、ビデオ、または静止画像を含み、前記サンプルの各々が値を有し、この方法が、前記コンテンツの少なくとも所定のサンプルを変化させて、これにより前記コンテンツ中の前記補助データの所定のビットを符号化するステップを含み、前記コンテンツを相補的領域に変換せずに前記符号化を達成する方法において、

前記コンテンツ内の所定の特徴を検出するステップと、

前記特徴に対応するサンプルを識別するステップと、

前記識別したサンプル、あるいは前記識別したサンプルの所定の近傍内のサンプルを変化させて、前記符号化を実行するステップと

を具えていることを特徴とする補助データの符号化方法。

【請求項２】　前記特徴が、隣接サンプルの近傍に関連する属性であることを特徴とする請求項１に記載の方法。

【請求項３】　前記変化が、前記ビット及び変化させるべき前記サンプルの元の値に従って変化させるものであることを特徴とする請求項１に記載の方法。

【請求項４】　前記変化が、前記ビットに従って変化させて、変化後の値が、近傍のサンプル値と所定の関係を有するようにするものであることを特徴とする請求項１に記載の方法。

【請求項５】　前記所定の特徴が、第１しきい値を超える値を有するサンプルであり、かつ前記サンプルと近傍のサンプルとの差が、所定しきい値以内の値を有することを特徴とする請求項１に記載の方法。

【請求項６】　前記近傍のサンプルが隣接サンプルであることを特徴とする請求項５に記載の方法。

【請求項７】　前記変化が、前記補助データのエネルギをスペクトル的に拡散させるものであることを特徴とする請求項１に記載の方法。

【請求項８】　前記識別したサンプルに隣接するサンプルを変化させるステップを具えていることを特徴とする請求項１に記載の方法。

【請求項９】　請求項１から請求項８までのいずれかに記載の方法を実行するコ

ンテンツ保護システム。

【発明の詳細な説明】

【０００１】

（発明の属する技術分野）

本発明は信号処理の分野に関するものであり、特にオーディオ、ビデオ、及び他のコンテンツを、ディジタル著作権管理目的で符号化するのに有用な技法に関するものである。

【０００２】

（発明の背景）

近年、電子情報の利用が爆発的に増加するのに伴い、著作権号の強化がより困難になってくる。音楽、美術、及び他の有価値の情報を表現するディジタルデータをコピーするのに必要な装置のコストが低下しつつあり、直ちに利用可能なデータ記憶媒体の容量が増加しつつある。廉価な装置が大量のデータを、書込み可能コンパクトディスク（ＣＤ－ＲまたはＣＤ－ＲＷ）、マルチーギガバイトのハードディスク装置、大容量リムーバブル磁気ディスク、および近々利用可能なディジタル多機能ディスク（ＤＶＤ）のようなディジタル記憶媒体に書き込むことができる。直ちに利用可能な高解像度のプリンタ及びスキャナが、グラフィック情報のディジタル化及び再生を、大部分の消費者が手の届く所にもたらす。これに加えて、直ちに利用可能な、アナログーディジタル及びディジタルーアナログ変換器を具えた高解像度のサウンドカードが、オーディオ情報のディジタル化及び再生を、大部分の消費者が手の届く所にもたらす。ディジタルファイルをコピーすることが簡単かつ廉価であるだけでなく、インターネットが著作権利化された作品の無認可の配布を促進している。

【０００３】

常に原本に劣るアナログのコピーとは異なり、ディジタル情報のコピーは、コピーによる劣化がなく、原本と同等になりうる。違法であるが正確なディジタルメディアの複写、及びアナログメディアのほぼ正確な複写によって、年間何百万ドルもの損失がある。コピー装置が直ちに利用可能なので、無認可のコピーを作成している人物を摘発することが困難になりうる。たとえ無認可のコピー者を逮捕しても、無認可の疑いのあるコピーが、実際に自分のオリジナル作品からコピ

ーされたものであり、独自に創作されたものではないことを、元のドキュメントの創作者が証明しなければならない。

【０００４】

（発明の開示）

以下に詳細に説明する本発明の一つの要点は、ディジタル透かし、あるいは「データ隠蔽」に関するものであり、そして違法コピーの問題解決にこれを利用することに関するものである。原データ中に補助情報を隠蔽することは通信秘匿とも称され、何千年もの間使用されてきている。通信秘匿では、他の物体または媒体内にメッセージを隠して、このメッセージが人間の観測者（または聴取者）に本質的に知覚されないようにする。通信秘匿は暗号化法と関係があるがこれとは異なるものであり、暗号化法では、メッセージが存在することは通常明らかであるが、特別な知識なしではその意味を確認することができない。

【０００５】

隠しデータは補助データまたは埋め込みデータとも称され、原データコマンド中に埋め込むことによって無認可のコピーを防止するのに用いることができ、これはコピー装置によって読み取り可能であり、かつコピー装置に使いものになるコピーを作成しないように指示するものである。また隠しデータは、データを認証するため、即ち原作者であることを証明するために用いることもできる。こうした技法の一つは、秘密アルゴリズムまたは暗号のように、補助情報を検出及び／または除去するのに特別な知識を必要とするような方法で、元の作品中に補助情報を埋め込むものである。コピー者が認証情報を除去することは不可能であり、埋め込み情報を復帰させることによって、その人が原作者であることを証明することができ、この埋め込み情報は、原作者を著作者として識別するものである。

【０００６】

データ隠蔽は、無認可コピーの防止及び検出以外にも使い道がある。こうした使い道の一つがコンテンツの拡張であり、即ち原データに情報を追加してコンテンツを拡張することである。例えば、ＣＤ上のオーディオデータ中に歌詞を埋め込むことができる。この歌詞は特別なカラオケ装置で見ることができ、オーディ

オは既存のＣＤプレーヤで再生することができる。また隠しデータは、ビデオデータの異なるセグメントを、ＤＶＤ上のビデオの、視聴者が選択可能な異なるバージョンに関連付けるために用いることができる。例えば視聴者が、子供用に編集したバージョンまたは無修正のバージョンを選択することができ、埋め込まれた補助データが、どのビデオセグメントをスキップして、どれを選択したバージョンに含めるべきかを、ＤＶＤプレーヤに指示する。

【０００７】

補助データを隠蔽した原データは、表現装置の助けにより知覚可能ないずれの種類の情報を表現することができる。例えばこのデータは、コンパクトディスクプレーヤまたはオーディオＤＶＤプレーヤを用いて演奏される音楽、ＤＶＤプレーヤで上映されるビデオ映画、あるいはコンピュータスクリーンまたはプリンタに表示される画像を表現することができる。

【０００８】

通常の表現装置によって、補助データ組込み済みのデータをユーザに対して表現する際には、補助データが原データの使用を妨害しないようにすべきである。理想的には、ユーザが補助データを全く知覚できないようにすべきである。不都合なことに、埋め込み補助データの量またはその強固さ、即ち攻撃またはデータ変更に対する耐性を増加させると、その知覚性も同じくらい増加する。ユーザに不都合な衝撃を与えずに補助データが知覚されうる程度は、アプリケーションによって異なる。例えばＣＤ品質のオーディオでは、原データからの微小な変化が、許容外の可聴歪みとなりうる。ビデオデータでは、上映される画像中の微小な変化は、たとえこの変化が、元の作品と補助データ組込み済みの作品とを並べて上映し比較して気がつきうるものであっても、許容しうるものでありうる。

【０００９】

元のディジタルデータ中に補助情報を隠蔽することについては、いくつかの技法が知られている。原データに付加したヘッダまたはトレーラとして、原データ中にデータを隠蔽することができる。フォーマットを変更する際に、補助データの位置を容易に発見してコピーから取り除くことができるので、こうした技法は著作権利化された作品の保護において限定的に使用される。より巧妙な技法は、

補助データを原データ中に分布させて、補助データを識別して、補助データ組込み済みのデータから取り除くことが困難になるか、あるいは統計的に不可能になるくらいまで、補助データと原データを絡み合わせる。

【００１０】

補助データを原データ中に分布させるデータ隠蔽技法の大部分は、演算が高密度であり、従って実現するには高価である。これらの技法の多くものもは、擬似ランダムノイズ（ＰＮ）列の期間を、補助情報を表現する信号と共に加算または減算することにもとづくものであり、これらの列は周波数領域でのフィルタリング（シェイピングとも称される）を必要とする。これらの技法の残りのものは、例えばフーリエ変換によってもとのデータを周波数領域に変換した後に、原データに補助情報を加算するものである。周波数領域で補助情報を加算して、ＰＮ列の方法と類似の方法で、補助データのエネルギが多くの周波数に広がるようにすることができる。これに加えて、補助情報を各周波数間に広げるか広げないかして、補助情報を周波数成分の位相に加えることができる。不都合なことに、データを周波数領域に変換すること、及びまたはＰＮ列が知覚されにくいようにＰＮ列のエネルギをシェイピング（整形）することは、瞬間的な演算を必要とする。

【００１１】

ユーザが補助データを検出する能力は、そのデータだけでなく、人間の感覚器の特性及び脳による感覚的刺激の解釈にも依存する。一部のデータ隠蔽技法は、原データを周波数領域に変換して、原データの周波数スペクトルが埋め込みデータの知覚性を低減するような方法で補助データを埋め込む。原データの周波数分布は、埋め込んだ補助データが知覚されにくくなるような、即ちマスクされるような好適な周波数を特定するために用いる。他の方法は、周波数領域では我々が位相を振幅ほど正確には知覚しないということを利用する。

【００１２】

演算密度がさほど高くないが、原データ中に補助データを分布させるいくつかのデータ埋め込み技法が存在する。こうした技法には、振幅変調、周波数帯の除去、個別量子化、及び最下位ビット（ＬＳＢ）の置換が含まれる。これらの技法は、原データとは無関係にデータを所定位置に埋め込むものであり、従って補助

データ組込み済みのデータにおける知覚的副作用がより生じやすい。これに加えて、ＬＳＢ置換技法は低レベルのノイズによって容易に妨害されやすい。

【００１３】

埋め込みデータを復帰させることの容易性は、埋め込みに用いる技法によって異なる。一部のデータ隠蔽及び復帰の技法は、補助データ組込み済みのデータと原データとを比較することによって補助データを復帰させる。他の技法は、データを隠蔽するために使用したＰＮ列のデータベースを用いて、補助情報を復帰させる。補助データを抽出するために、原データのコピーまたはＰＮデータベースを使用することが必要な技法は、補助データ組込み済みのデータが広範に分布するようなアプリケーションにおいて限定的に使用される。こうした技法は、著作権保有者ぐらいしか補助データの復帰を行わないようなデータ認証のような一部のアプリケーションでは有用である。

【００１４】

埋め込みデータ技法は次のいずれかの理由により、補助情報の除去に影響されやすい。第１には、埋め込みデータの性質そのものが、ＭＰＥＧ圧縮で行うようなデータの非知覚性の要素を除去するビットレートの低減（圧縮とも称される）方法と整合しないということである。いずれの埋め込みデータのキー的特徴も非知覚性であるので、圧縮方法が埋め込みデータを除去するように作用する。たとえ現代の圧縮技術を免れるように埋め込みデータを設計しても、次世代の技術ではおそらく除去されてしまう。メディアのディジタル配布ではビットレート圧縮が非常に重要であり、研究が行われている。第２には、ノイズ低減技法が新しい話題であり、旧来の記録を復旧するために用いられているということである。大部分の非知覚性の埋め込みデータがノイズと類似しているので、これらのノイズ低減技法によって除去されてしまう。ここでも、たとえ現代の復旧技術を免れるように埋め込みデータを設計しても、次世代の技術ではおそらく除去されてしまう。

【００１５】

以下に詳細に説明する本発明の他の要点では、本技法は改ざん及び攻撃に対してより強固にする方法及びシステムに関するものである。

【００１６】

埋め込みデータは種々の改ざん及び攻撃を受けやすい。例えば、埋め込みデータ技術の性質そのものが、ＭＰＥＧ圧縮で行うようなデータの非知覚性の要素を除去するビットレート低減（圧縮とも称する）方法と合わない。大部分の埋め込みデータの特徴が非知覚性であるということなので、圧縮方法が埋め込みデータを除去しがちである。たとえ現代の圧縮技術を免れるように埋め込みデータを設計しても、次世代の技術では除去されるようになりうる。メディアのディジタル配布ではビットレート圧縮方法が非常に重要であり、さかんに研究が行われている。同様に、例えば旧来のオーディオ録音を復旧するために用いるようなノイズ低減技法が、埋め込みデータに脅威をもたらす。大部分の非知覚性の埋め込みデータがノイズと類似しているので、これらのノイズ低減技法によって除去されてしまう。ここでも、たとえ現代の復旧技術を免れるように埋め込みデータを設計しても、次世代の技術ではおそらく除去されてしまう。

【００１７】

以下に詳細に説明する本発明の他の要点では、本技法はＩＤ割り当て及び拘束に関するものである。コンテンツ供給者は、コンテンツを購入した人だけに、このコンテンツにアクセス（即ち再生、コピー、または記録）することを許可したい。これを行うための一つの方法は、ＩＤを含むコンテンツを提供して、消費者、表現装置、または記憶装置に対してＩＤをロックすることである。しかし、ＩＤの使用法であるこれらの既存の解決法は、消費者に不合理な負担をもたらす。

【００１８】

ユーザ拘束として知られている一つの既存の解決法は、コンテンツにアクセスするために、ＩＤカードを携帯すること及び／または個人識別番号（ＰＩＮ）を覚えていることを人に要求するものであり、銀行のＡＴＭ機の動作に類似している。銀行にある預金にアクセスするために、消費者はこの解決法を受け入れており、この状況では、消費者にとっても安全性が利点である。しかし、例えばオーディオをカーステレオで再生するようにコンテンツにアクセスするために、こうした要求を消費者が受け入れるかは疑問である。これに加えて、人のグループが音楽のようなコンテンツを共用する際に、音楽を聴く前にカードをスキャンさせ

なければならないという各人のプロセスは、押し付けがましいものである。最後に、この解決法はＩＤをユーザに結び付けるデータが必要であり、このためＰＩＮ及び／またはＩＤカードが生じうる。このデータは、ユーザがプライバシーについて譲歩していることを意味する。

【００１９】

他の既存の解決法は、コンテンツの再生を１台の装置に限定するというものであり、プレーヤ拘束として知られている。この解決法は、友人の持つ音楽を自分のカーステレオで再生することも、自分の映画を友人の家で再生することもできないことを意味する。この解決法は消費者に不都合であるばかりでなく、多くの人が再生した後に、あるいは友人と視聴した後にコンテンツを購入するので、コンテンツの売上も低減させるものである。

【００２０】

最後の解決法は、コンテンツを記憶装置に結び付けるものであり、メディア拘束として知られている。これらの記憶装置は磁気ディスクドライブ、光ディスク装置、または電子メモリを含むが、これらに限定されない。コンテンツを他の種類の記憶装置間での移動を許可すべき際に、この解決法は邪魔なものとなる。例えばジョーというユーザが、自分のコンピュータのハードディスクから自分のホームステレオでオーディオを再生したい、あるいはオーディオを携帯電子メモリとして自分のカーステレオまたはジョギングに持っていきたいことがある。しかし、このメディア拘束の解決法では、このオーディオを一箇所でしか再生できず、このオーディオをジョーのステレオから彼の車に持っていくためには、彼はこのオーディオをどこに対して「チェックアウト」したかを覚えていなければならず、さもなければ海賊行為（著作権侵害）を規制することができない。重要なことは、単に消費者が所望する各箇所でオーディオを聴くことさえもできないということである。

【００２１】

以下に詳細に説明する本発明の他の要点は、権利管理機能を実行するために、異なる特性を有する多数の埋め込みデータの使用を含むものである。

以下に詳細に説明する本発明の他の要点は、コンテンツをスクランブルして権

利を保護することに関するものである。

【００２２】

ディジタル信号を劣化させて、アクセスを制限することが往々にして望ましい。例えば、有料テレビ放送では、番組に対して未払いの人にとっては、映像が不鮮明なのでこれを見られないほどに劣化させ、番組に対して支払い済みの人にとっては、自分の復元装置が動作可能であり、鮮明な画像が見られるようにする。ごく最近では、ディジタルオーディオ革命の結果として、ＭＰ３（標準ビットレート圧縮のオーディオファイルフォーマット）のアクセスを制限することが望まれている。廉価な携帯ＭＰ３プレーヤを生産することも望まれており、これは反対に、原信号の復元が簡単であることが要求される。

【００２３】

ディジタルコンテンツを劣化（スクランブルとも称する）させる既存の方法は多数ある。一部の方法はコンテンツをスクランブル解除するためのキーを必要とし、他のものは必要としない。大部分のスクランブルまたは劣化方法は、妨害信号をディジタルコンテンツに加えるか、あるいはビットを周回させるかのいずれかにもとづくものである。他の方法は暗号化を用いるものであるが、これは演算が非常に高密度である。

【００２４】

スクランブルしたチャネル上の映画についての情報を、スクランブル解除する必要なく視聴者に表示することができれば有利である。

【００２５】

かなり最近、ディジタルオーディオ革命の結果として、コンテンツの正確なディジタルコピーを作成することが容易になったので、一部の人たちはＭＰ３（動画の専門家グループの階層IIIの規格のビットレートを低減したオーディオフォーマット）アクセスを制約のあるものと見るようになった。この制約はスクランブル技術によって実現されている。しかし、歌を演奏するか否かを決める前に、ユーザが歌について知ることができるようになり、このためユーザにとってのシステムのスピードが向上するので、スクランブルされた歌についての情報をスクランブル解除せずに、この情報を復元できることが望ましい。このことは、ユー

ザのプレーヤが、再生を可能にする著作権情報を迅速に読み出すことも可能にする。また、廉価な携帯ＭＰ３プレーヤを生産することも望ましく、ここでは逆に、原信号の復元が簡単であることが必要である。

【００２６】

多数のスクランブル及びスクランブル解除の方法が、従来法に含まれる。しかしこれらの方法は、スクランブル及びスクランブル解除のプロセス中にヘッダ情報をそのままにしておくように設計されたものではなく、このためこれらの方法は、すべての情報をスクランブル解除せずに、スクランブルしたオーディオについての情報を復元することは不可能である。

【００２７】

以下の詳細な説明は、以上で挙げた種々の論点について記述したものであり、これらの問題うちのいくつかを是正し、以上に挙げていない新たな機能を提供するものである。

【００２８】

（実施例の詳細な説明）

データ隠蔽装置の紹介

以下、本発明の実施例について図面を参照して説明する。以下の説明は、好適な具体化、方法、及び動作の特徴図面を参照して進める。以下に挙げる例のうち、明示的に説明したもの、あるいは合理的に示したもの以外は、他の構成を排除すべきものではない。

【００２９】

１つの実施例によれば、コストの低減を伴った高効率をもたらすデータ隠蔽及び復帰の方法及び装置が提供される。一部の実施例では、精神物理学的なデータ隠蔽を用い、データを隠すべき位置を識別するために、原データを修正または変更する必要がない。特定の実施例では、符号化により、本質的にコンテンツの統計量を変化させずに、隠し信号を識別及び除去しにくいままにすることができる。

【００３０】

ユーザが、知覚性、強固さ、及び埋め込みレートを変化させるようなパラメー

タを設定でき、開示した技術を多種多様なアプリケーションで使用できるように、本発明を実現することができる。

【００３１】

好適な装置は、標準的なパーソナルコンピュータまたはＤＳＰボードにあるような、論理プロセッサ及び記憶装置を具えている。これらの装置はデータ読み取り器、比較器、及びデータ書込み器として作用して、ユーザが所望する透かしの埋め込み及び／または復帰をすることができる。

【００３２】

好適なプロセスは、補助的な情報を原データ中への埋め込み及び復帰を行って、補助情報組込み済みのデータを生成することを含む。１つ以上の検出基準を用いて、原データ中の、データ点の位置特定及び／または調整を行う箇所を決定して、補助情報が載るようにする。この検出基準は、他の簡易なプロセスに比べて、補助データの埋め込みがより知覚されにくくなるような、原データ中の位置（局所的マスキングの機会と称する）を発見するために用いることができる。

【００３３】

補助データを埋め込む際に、前記検出基準に従い原データ中のデータ点を調査して、局所的マスキングの機会の存在を特定する。これらの検出基準は、例えばデータ点を所定値と比較すること、及びこのデータ点の近傍点との関係を検査することを含む。検出基準に合う場合には、１つ以上の近傍点、あるいは調査すべきデータ点を、補助データの埋め込みビット値を示すように変化させる。

【００３４】

こうして、局所的マスキングの機会の探索は通常、データ中のデータ点毎に進めるが、各点の調査には、この点の値だけでなく、１つ以上の近傍点の値、及び／または１つ以上の点どうしの関係も含める。データ点の調査により局所的マスキングの機会の存在が示された場合には、１つ以上の局所点、即ち調査中の点または１つ以上の近傍点の値を設定することによって、データを埋め込む。

【００３５】

実施例において近傍データ点に設定する値は通常、調査中のデータ点、並びに補助データビットの値に依存する。データ点の値が近傍のデータ点と特定の関係

があるように、データ点の値を設定することができる。原データを通して調査し尽くすまで、あるいはまだ埋め込まれたままの補助データがなくなるまで、このプロセスを継続する。

【００３６】

補助データの復帰は、埋め込みプロセスの逆である。前記検出基準を用いて、補助データ組込み済みのデータを通して調査して、局所的マスキングの機会の位置を見出す。各局所的マスキングの機会の位置を見出す毎に、近傍データ点あるいは埋め込みビットを示すべく設定した点を読み込んで、埋め込みデータを抽出する。補助データ組込み済みのデータを調査し尽くすまで、このプロセスを継続する。

【００３７】

好適な実施例では、絶対的な値でなく、近傍データ点と相対的な値にデータ点を設定する。原データに無関係な値にデータ点を設定することよりもむしろ、局所的マスキングの機会にデータ点を設定すること、及び近傍点に関係する値にデータ点を設定することの方が共に、データの知覚性を低減するマスキングをもたらす。局所的マスキングの機会の近傍の点の関係または値を特定することによって、データを抽出することができる。

【００３８】

以下に詳細に記述する２つの好適な実施例については、大きな値を有する点のみを最小量だけ調整するものであり、よってこれらの実施例は、強い刺激によって弱い刺激がマスキングされることにもとづくものである。このプロセスはアナログ及びディジタルデータに適用可能である。しかし、現代のディジタルメディアへの切り替わり、及びわかりやすさのために、両実施例ともディジタルメディアで説明する。

【００３９】

特に第１の好適実施例は、ピークが大きなしきい値を上回り、かつピークと次の点との間の元々の差が過大でない限り、ピーク後のデータ点と補助情報を載せるべきピークレベルとの差を利用するものである。この大きなしきい値及び最小差により、所望の知覚的マスキングがもたらされる。この埋め込みプロセスは、

しきい値を超えるピーク後の点を調整して、補助データを隠蔽するものである。これに対応して、復帰プロセスはしきい値を超える各ピークと次のデータ点との差を測定して、補助データを復帰させるものである。

【００４０】

第２の好適な実施例は、元の傾斜の変化が過大ではないが、確実にするための調整を受けるのに十分なくらい急峻である限り、大きく急峻な正のしきい値交差間の傾斜の変化を利用して、補助情報を隠蔽するものである。ここでも、大きなしきい値によって所望の知覚的マスキングが行われる。実現に当たっては、埋め込みプロセスが傾斜の変化を調整してデータを埋め込み、復帰プロセスが傾斜の変化を測定して補助データを得る。

【００４１】

通常、好適な埋め込みプロセスは、補助情報のエネルギを原データ中に、スペクトル的に暗に拡散させる。この広帯域の方法は、可聴外の周波数範囲にデータを配置するサブバンド（副帯域）の方法よりも、除去することがより困難なデータを生成するものである。所望すれば、このプロセスが、マスクされていないデータと統計的に同等な保護されたデータを生成するようにパラメータを選定することができる。知覚、符号化レートと攻撃に対する強固さとの間に所望のトレードオフが成り立つように、このプロセスを調整できることが重要である。

【００４２】

こうした実施例は、本質的にではないが、フーリエ変換のような複雑なデータ変換を必要とせずに、原データ上で動作することが好ましい。このため、原データが時間領域で情報を表現する場合には、補助データの埋め込み及び復帰を行う間に、このデータを時間領域に留めることができる。もちろんこの技術は、例えば周波数領域または時間領域のように、すべての種類の原データ上で動作させることができる。例えば、ＭＰＥＧ１及びＭＰＥＧ２仕様、ＩＳＯ11172-3及びＩＳＯ13818-7を含むＭＰＥＧデータにこれを適用することができる。

【００４３】

最後に、圧縮として知られているビットレート低減技法の問題では、圧縮（符号化とも称する）及び伸長（復号化とも称する）中に、別個であるができれば同

等の透かし手続きを用いることによって、透かしの除去をとばすことができる。

【００４４】

好適な具体化及び方法

一実施例によるシステムは、原データ中に補助情報（またはデータ）を隠蔽する方法及び装置、及びこの補助情報を復帰させる方法及び装置から構成される。

【００４５】

図１に、データを埋め込む方法の例の実行に含まれるステップの概要を示す。図２に、図１の方法を実行するために使用しうる装置１０のブロック図を示す。装置１０はマイクロプロセッサ１４を具え、これは例えば、パーソナルコンピュータまたはエンジニアリングワークステーションの、インテル社のPentium(登録商標)またはＤＥＣ社のAlphaのような汎用マイクロプロセッサ、あるいはテキサスインスツルメンツ社のTMS320ラインナップのようなディジタル信号プロセッサ（ＤＳＰ）、あるいはメディアプロセッサまたはカスタムの処理回路のような専用ＣＰＵとすることができる。装置１０は記憶装置１８も具え、これはランダムアクセスメモリ（ＲＡＭ）または遅延回路を含むことができる。本実施例で用いるアルゴリズムは演算密度が高くないので、１秒当たり100万命令未満のオーダの演算が必要であり、近代の大部分のパーソナルコンピュータによって実行することができ、そしてこれより能力の低い装置（例えばパーソナルディジタル補助器具、専用メディアプレーヤ、等）でも実行することができる。

【００４６】

以下に述べる原データは、振幅を周期的にサンプリングすることによって録音した音を表現することができ、各サンプルは２進数を用いて特定時刻の音の振幅を表現する。同様に、これらのサンプルは画像またはビデオの画素を表現することができる。さらに原データは、グループにまとめられるいずれの２進データの列とすることもできる。同様に、補助情報は「１」及び「０」として表現可能ないずれのデータでもありうるが、開示した装置を対応させて適用すれば、他の文字記号も同様に用いることができる。

【００４７】

図１に示すように、ステップ２０では、原データの一部を図２の記憶装置１８

に読み込む。ステップ２４は、論理プロセッサ１４によってサンプルデータを順次調査して、所定の検出基準に合うサンプル点の位置を見出すことを示す。この検出基準は、補助データを埋め込むべき点またはその近傍での、１つのサンプルまたは２、３のサンプルの値の変化が通常、音の聴取者によって知覚可能な最小のものになるようなものなので、こうしたサンプル点は「局所的マスキングの機会」の存在を示す。マスキングの量は、データの種類及びユーザが選択した設定による。例えば、非圧縮のオーディオに対してはマスキングが大きくなり、ＭＰＥＧのようなビットレートを低減した（ディジタル的に圧縮した）データに対してはマスキングが小さくなる。データの復帰中にも同じ検出基準を適用して、隠しデータの位置を見出すことができる。

【００４８】

原データの各点を調査して、この点が局所的マスキングの機会を表現するか否かを特定することが好ましい。局所的マスキングの機会を特定する基準は、調査中の点の値だけでなく、少なくとも１つの近傍または隣接点の値、あるいは近傍点と調査中の点との関係も含めて課することができる。この検出基準は、例えば、調査中の点が所定のしきい値を超えること、及び／またはこの点が、１次導関数または高次導関数において、局所的に最大の点であることを必要としうる。この基準は、調査中の点に後続する点が、調査中の点とは所定量未満だけ異なる値を有するか、あるいは調査中の点との間に他の関係を有するという要求を含みうる。

【００４９】

サンプルデータ点は、例えば時間をｘ軸に、サンプルの大きさをｙ軸にとって、グラフにプロットされるものと考えることができる。このため、一連のデータ点はいずれの点の間にも傾斜を有するものと考えられ、この傾斜の値を検出基準の一部とすることができる。この基準は例えば、調査中の点及び先行する点によって規定される傾斜が特定値を超えるということか、あるいは点の前後での傾斜の変化が特定値を超えないということを指定することができる。この基準は、あらゆる要求の組合わせを含むことができ、これらの詳細例は本質的なものではなく、本発明の範疇を限定するものでもない。

【００５０】

これらの例の場合には、補助データをマスクするために複雑なデータ変換が必要でなく、従ってデータ点と検出基準とを比較することは、比較的迅速かつ廉価に行える。離れた点を用いて原データを周波数領域に変換して、埋め込みデータをマスクする方法を決定する多くの従来法とは異なり、本実施例は近傍点または隣接点、即ち有用な周波数データの決定に用いるには近すぎる点のみを用いてマスキングの機会を特定する。近傍点は、調査中の点の隣の点、あるいは比較的少数の点以内の点を含み、これは50点以内であることが好ましく、20点以内であることがさらに好ましい。この基準は、データ点がしきい値を超えるか否かを特定できるくらいに簡単にすることができる。

【００５１】

ステップ２６は、検出基準に合う点の位置を見出した際に、局所的マスキングの機会の付近の特定のサンプル点の値が、埋め込むべき補助情報の値を反映するように変化していることを示す。変化したサンプルは単に、埋め込みビットの値を表わすような特定値に設定されたものでありうるが、新たな値は通常、補助データの値及び近傍点または局所的マスキングの機会を検出するために調査した点の値に共に依存する。例えば、値または傾斜の変化が、埋め込みビットが「１」か「０」か（または他の記号）を表わすように点を設定することができる。

【００５２】

点が新たな値に設定される際に、前記変化が、元のサンプル点が検出基準に合い続けることの妨げにならないか、あるいはこの局所的マスキングの機会をとばして復帰プロセスで検出されないようにするかのいずれかが好ましい。さもなければ、埋め込んだ補助データが復帰不能になりうる。

【００５３】

あるいはまた、単に補助ビットを最下位ビットまたは他のビット、好適には下位ビットとして埋め込むことも可能である。例えばデータが所定しきい値より大きいことのような局所的マスキングの機会を表現するように埋め込みビットの位置を選定したので、この埋め込みビットはマスクされたままである。

【００５４】

ステップ３０は、さらに補助データを埋め込む必要がない場合に、ステップ３２でプロセスを終了することを示す。さもなければ、ステップ３４は、まだデータがメモリに存在する場合には、局所的マスキングの機会の探索を継続することを示す。ステップ３６は、メモリの全データをまだ探索していない場合には、さらにデータをメモリに読み込むことを示す。メモリのデータの始点または終点で生じる局所的マスキングの機会を失わないために、メモリ内のデータを一部重複させる必要がありうることは、当業者には明らかである。

【００５５】

図３に、復号化方法の実行に含まれるステップを大局的に示す。データを埋め込むために用いたのと同じプロセッサ及びメモリを、データを復帰させるために用いることができるので、図３の各ステップは、必ずしもそれだけではないが、図２のハードウエア構成要素を用いてデータを抽出することを記述したものである。ステップ５０は、補助データ組込み済みデータの一部を記憶装置１８に読み込むことを示す。ステップ５２は、論理プロセッサ１４が各データ点を調査して、局所的マスキングの機会を特定することを示す。サンプル点が局所的マスキングの機会の基準に合う場合には、ステップ５４は、補助データを埋め込んだ方法と逆の関係を用いて、埋め込んだ補助データの「１」または「０」ビットを抽出することを示す。ステップ５６は、まだ補助データ組込み済みのデータがメモリにある場合には、ステップ５２で論理プロセッサが残りの点の調査を継続することを示す。ステップ５８は、メモリのすべてのデータを調査し尽くしたが、未調査の、補助データ組込み済みのデータがデータファイル中にある場合には、ステップ５０でさらにデータをメモリに読み込むことを示す。ステップ６０は、すべての補助データ組込み済みのデータを調査し尽くすとプロセスを終了することを示す。

【００５６】

ここで２つの特定の実施例について簡単に説明し、その後に、この方法の利点について詳細に説明する。図４に示すように、第１実施例は大きな正のピークを検出基準１２０として用いて、このピークと次の点との間に補助情報を記憶するものである。図７に示すように、第２実施例は、傾斜の変化が最小の、大きく急

峻なしきい値交差を検出基準１４０として用いて、補助情報１５０を傾斜の変化に載せる。

【００５７】

この方法はアナログまたはディジタルデータに適用可能であるが、好適な実施例ではディジタルデータを用いている。例えば、アナログデータをナイキストレートでサンプリングして、追加的情報が隠れているディジタルデータを生成する。そして、ディジタル信号処理（ＤＳＰ）における何らかの既存の方法によって、追加的情報が組み込まれたディジタルデータをアナログ領域に戻すことができる。ここでは、このアナログデータは埋め込みデータを含んでおり、これはサンプリングを用いて復号化することができる。これは上述した方法でアナログデータを符号化する方法の１つの可能性に過ぎない。

【００５８】

この方法は、オーディオ、音声、画像、ビデオ、または他のいずれの知覚可能な信号にも適用可能である。オーディオ及び音声については、原データが圧力－時間、振幅－周波数、あるいは特定周波数の大きさ－時間を表現しうる。画像については、原データがグレーコード－空間、分離または結合したＲＧＢまたは同等のもの－空間、あるいは振幅－周波数を示す。ビデオデータは、利用可能な時間の時限を加えた画像データを含むものである。例えば、ＭＰＥＧでビット低減したオーディオまたは画像では、スケールファクタまたは周波数係数－周波数または時間、あるいはその両方の形で、補助データを埋め込むことができる。

【００５９】

通常、検出基準のうちの１つは大きいしきい値である。16ビットのオーディオでは、最小値より上の48dBより大きいしきい値が望ましい。このしきい値は、マスキングによる最小知覚でデータが変化しうるようにする。マスキングは、定常状態の刺激のしきい値の増加として定義されている心理学用語である。本明細書ではこの用語を、前記定義よりずっと広義に用い、一組のデータが、他のデータに対する知覚を低下させる様子を表わす。特に、非圧縮の振幅－時間データについては、入力レベルの増加に伴いセンサ系の感度が低下して、これにより隣接データ点の微小な調整が、しきい値の大きな値によってマスクされる。ＭＰＥＧデ

ータのような、ビットレートを低減した時間－周波数データについては、マスキングが最小であり、ビットレートを低減するために既にマスキングを使用しているので、教科書的定義により似ている。

【００６０】

最後に、この方法は、マスキングを使用していないデータに適用可能であるが、補助情報を復帰させるために、ＰＮ列または原データのようなキーを必要としないという点でプロセスの効率が優位である。まとめれば、検出基準のパラメータにより、データレート、プロセスの複雑度と知覚品質との相互関係が決まる。

【００６１】

実施例１

第１の特定実施例は、原データ中の大きいピーク内に補助情報を隠蔽するということにもとづくものである。本実施例では、補助情報をＮビットの語に分解して、より良好なエラー回復のために、同期データをこれらの語の間に置く。ノイズまたはファイル修正に対する強固さを必要としない場合には、この補助情報は語の間に同期パルスを含む必要がない。

【００６２】

図４に、第１実施例において、ピークまたは局所的な最小値を検出して、このピークに関連してその後の点の値を設定して、埋め込みビットの値を指示することを概念的に示す。

【００６３】

図５は擬似符号について、埋め込みプロセスのフローチャートの形で示す。このプロセスは、thrというラベルを付けた大きいしきい値の上にあり、ピークの後に、dSというラベルを付けた比較的小さい減少があるような正のピークを発見するまで、原データを探索することから始まる。このプロセスはボックス２００、２１０、及び２２０で表わす。この検出基準を、最も演算効率の高い順序でチェックし、ピークは最もふさわしくない基準なので、このチェックは、まず点がピークを表わすか否かを見極めるチェックを含む。

【００６４】

所望のピークを発見すると、ユーザ定義のビット深さｂによりピーク後のデー

タ点を調整して、補助情報を載せる。ボックス２４２、２３０、及び２５０に示すように、特に、このピークが補助語の始点である場合には、ピーク後の点x[n+1]がピークx[n]から、ピークと次の点との間に許容される変化の最大値の半分dS/2を引いたものに等しくなるように調整することによって、同期符号を埋め込む。ピーク後の点x[n+1]を、ピークx[n]から、ピークと次の点との間に許容される変化の最大値の半分dS/2を引いて、ビット深さの大きさの半分2^{b-1}を足したものに調整することによって、１の補助情報ビットを符号化する。これに対応して、ピーク後の点x[n+1]を、ピークx[n]から、最大変化の半分dS/2とビット深さの大きさの半分2^{b-1}の和を引いたものに調整することによって、０の補助情報ビットを符号化する。この０及び１の埋め込みは、ボックス２４２、２４０、２６０、２７０、及び２８０に示す。ボックス２９０に示すように、データを埋め込んだ次の２点を飛ばして、データの遅い（即ち平坦な）変化に対して他のピークが生じないようにすべきである。

【００６５】

ボックス２４２及び２４０で表わす補助情報を原データ中に隠し終えるか、あるいはデータが終わるまで、これらのステップを繰り返す。

【００６６】

図６に、擬似符号について、第１の特定実施例の復帰プロセスのフローチャートの形で示す。このプロセスは、thrというラベルを付けた大きいしきい値の上にあり、ピークの後に、dSというラベルを付けた比較的小さい減少があるような正のピークを発見するまで、原データを探索することから始まる。このプロセスは、ボックス３００、３１０、及び３２０で表わす。ここでも、効率を向上するために、まずピークを探索する。

【００６７】

所望のピークを発見すると、このピークとピーク後のデータ点との差を測定して、補助情報を復帰させる。ボックス３３０及び３５０に示すように、特に、ピークからピーク後の点を引いたもの、即ちx[n+1]－x[n]が最大許容変化の半分dS/2に近い場合には、新たな補助語の始点である。ピークからピーク後の点を引いたもの、即ちx[n+1]－x[n]が、最大許容変化の半分dS/2からビット深さの大きさ

の半分2^{b-1}を引いたものにほぼ等しい場合には、１の補助ビットを発見したことになる。この差、即ちx[n+1]－x[n]が、最大変化の半分dS/2とビット深さの半分2^{b-1}の和に近い場合には、０の補助ビットを復帰させたことになる。この０及び１の復帰を、ボックス３４０、３６０、３７０、３８０、及び３８２に示す。ボックス３９０に示すように、ピークを復帰させた後の２点を飛ばすことができる。

【００６８】

原データ中の補助情報を復帰し終えるか、あるいは原データが終わるまで、これらのステップを繰り返す。

【００６９】

しきい値thr、ビット深さb、及び傾斜の後の最大許容変化dSを含む３つのユーザ定義のパラメータが存在する。16ビットのオーディオについては、上述したように、このしきい値は通常、最小量子化値の約48dB上である。１サンプル当たりのサンプル数がより多いデータについては、このしきい値を増加して知覚を低下させることができる。ビット深さは、データを埋め込むためにサンプル点に生じる相対変化の指標である。このため、ビット深さが小さいほど、原データの妨害が小さく、埋め込みデータが聴取者により知覚されにくくなるが、より強固でなくなり、即ちノイズまたは攻撃によってより消失しやすくなる。ビット深さが１ビットから６ビットまでの間であれば、16ビットオーディオでの最小知覚が見出される。しかし、知覚的な劣化と引き換えにノイズに対してより強固であることを望めば、より大きいビット深さを用いることができる。ピーク後の最大許容変化dSは、少なくとも所望するビット深さの大きさ2^bでなければならない。一方では、dSをビット深さの大きさの２倍、即ち2^{b+1}に設定すれば、歪みが大きくなる犠牲を払って、ノイズに対する強固さをより良好にすることができる。他方では、統計的暗号解析（統計的に不可視とラベル付けした）で検出不能なようにしきい値を保つことを望めば、dSを2^bに設定して、bを小さく、おそらくは３ビット未満に設定すべきである。dSが2^bでない場合には、埋め込みをしたファイルと通常のファイルデータとの間での、大きな正のピークと次の点との平均差の相違を用いることができる。最後に、dSが2^bよりもずっと大きい場合には、デ

ータ埋め込みに適したピークがより多く発見されるので、補助情報の埋め込みレートを増加させる。上述した原理を用いて、当業者はユーザ定義のパラメータを、特定のアプリケーションの要求に適した値に設定することができる。

【００７０】

上述したように、通常、大きなしきい値によって、補助情報が加わることの知覚的効果が低減され、データの種類によっては、補助データを知覚不能にすることさえもできる。これに加えて、ピークでの０に近い傾斜により、データ変化が最小なので、多くのデータ点が、ピークとピーク後のデータ点との差が小さいということを満足する。この小さい差は、しきい値に比べて調整が小さくなり、このため埋め込み補助データが知覚される機会が減るということを意味する。

【００７１】

擬似符号について、前方予測力（即ちx[n+1]）と見られるものを有するバッファを用いて示す。これにより、プロセスがより説明しやすく、かつよりわかりやすくなる。しかし、n+1をkで置き換えて、直前の２点、即ちx[k-1]及びx[k-2]をたどっていくことによって定まるように、このプロセスは略式のものである。

【００７２】

最後に、ピークを定義するために、さらなる基準を追加することができる。例えばピークが、x[n]>x[n-2]、x[n]>x[n+2]、x[n]>x[n-3]、x[n]>x[n+3]、等の各方向に、より多くの点にわたって延在するか、あるいはピークが最小尖鋭度、即ちx[n]-x[n-1]>5のものである。ピーク基準の変化が補助データを埋め込むことができるレートに悪影響しても、ピークを移動することにより、より多くのノイズが取り除かれるので、これら基準の両者によって、ノイズに対する強固さがより良好になり、歪みが少なくなる。

【００７３】

原データ及びユーザ定義のパラメータによって、埋め込みデータ密度及びビットレートが異なる。例えばＣＤ品質のオーディオデータでは、ビット深さ５及びしきい値5000(74dB)を用いて、99～268ビット/秒のビットレートが達成される。ビット深さ８を用いて、しきい値5000を保てば、平均埋め込みレートは1000ビット/秒になる。ビット深さ８でしきい値を2000に下げると、平均埋め込みレート

が2000ビット/秒になる。

【００７４】

実施例２

第２の特定実施例では、大きく急峻なしきい値交差であり、かつ傾斜の変化が大きくないものに、補助情報を隠蔽する。この方法は、検出位置を変化させるノイズに対してより強固である。しきい値交差が通常、定義により０に近い傾斜であるピークにおける傾斜よりも大きい傾斜を有するため、ピークの位置に比べて、しきい値交差の位置がノイズによって変化しにくいので、こうしたことが起こる。本実施例ではオーディオデータでのテストを示し、これは第１実施例に比べて、ノイズに対する強固さと引き換えに、より低いデータレートとなり、かつより低いビット深さではより知覚されやすくなる。アプリケーションに応じて、おそらくは最適な実施例を見出すことができる。

【００７５】

図７に、しきい値交差での傾斜に関連させて、しきい値交差の後に傾斜を設定することによってデータを埋め込むことを、概念的に示す。

【００７６】

図８に、第２の好適実施例を用いて補助情報を隠蔽するための擬似符号について、フローチャートの形で示す。傾斜の変化（dSとラベル付けした）が最小の、大きく急峻な、正のしきい値（thrとラベル付けした）交差を発見するまで、原データを探索することからプロセスを開始する。このプロセスは、ボックス４００、４１０、及び４２０で表わす。

【００７７】

所望のしきい値交差を発見すると、ユーザ定義のビット深さ(b)により、このしきい値交差後のデータ点を調整して、傾斜の変化に補助情報を載せる。なお傾斜の変化は、(x[n+1]-x[n])-(x[n]-x[n-1])またはこれと同値のx[n+1]-2*x[n]+x[n-1]として定義する。ボックス４４２、４３０、及び４５０に示すように、特に、補助語の先頭である場合には、しきい値交差の後の点x[n+1]を調整することによって同期符号を埋め込んで、傾斜の変化が０になるようにする。しきい値交差後の点x[n+1]を調整して、傾斜の変化がにビット深さの大きさの半分2^{b-1} に

等しい分だけ正になるようにすることによって、１の補助ビットを符号化する。これに対応して、しきい値交差後の点を調整して、傾斜の変化がにビット深さの大きさの半分2^{b-1}に等しい分だけ負になるようにすることによって、０の補助ビットを符号化する。この０及び１の埋め込みは、ボックス４４２、４４０、４６０、４７０、及び４８０に示す。ボックス４９０に示すように、効率化のために、データを埋め込みの後の点を飛ばすことができる

【００７８】

補助情報を原データ中に隠し終えるか、あるいは原データが終わるまで、これらのステップを繰り返す。

【００７９】

図９に、擬似符号について、第２の好適実施例における補助情報の復帰のフローチャートの形で示す。このプロセスは、大きく急峻な、正のしきい値（thrとラベル付けした）交差を発見するまで、原データを探索することから始まる。このプロセスは、ボックス５００、５１０、及び５２０に示す。

【００８０】

所望のしきい値交差を発見すると、しきい値付近の傾斜の変化を測定して．補助情報を復帰させる。ここでも傾斜の変化は、(x[n+1]-x[n])-(x[n]-x[n-1])またはこれと同値のx[n+1]-2*x[n]+x[n-1]として定義する。ボックス５３０及び５５０に示すように、特にしきい値交差の傾斜の変化がほぼ０である場合には、新たな補助語を開始する。しきい値交差の傾斜の変化が、ビット深さの大きさの半分2^{b-1}にほぼ等しい正の変化である場合には、１の補助ビットを発見したことになる。しきい値交差の傾斜の変化が、ビット深さの大きさの半分2^{b-1}にほぼ等しい負の変化である場合には、０の補助ビットを発見したことになる。この０及び１の復帰は、ボックス５４０、５６０、５７０、５８０、及び５８２に示す。ボックス５９０に示すように、効率化のために、データを復帰させた後の点を飛ばすことができる。

【００８１】

原データ中の補助情報を復帰させ終えるか、あるいは原データが終わるまで、これらのステップを繰り返す。

【００８２】

上述したように、埋め込みプロセスが、検出基準を満たすことから埋め込み位置を除いてほしくない。特に本実施例では、ボックス４２０及び５２０の検出しきい値における、しきい値前の変化条件、即ち$x[n]-x[n-1]>dS+2^{b-1}$は、次のデータ点の調整が、この点をしきい値の下に戻さないことを要求する。代案の方法は、この条件を無視して、埋め込みプロセスが次の点をしきい値の下に移動させる場合には、現在または次の点（それぞれx[n]またはx[n+1]）のいずれかをしきい値に設定して、埋め込み及び復帰の両プロセスにおいて、しきい値に等しいあらゆるデータ点を無視することである。面白いことに、埋め込み時のみに、同期または０が、次の点をしきい値より下に移動させうる。これらの選択肢が与えられれば、プロセスが略式のものであり、このため略式プロセスの既知の利点を具えるように、記述した実施例を選定することができる。

【００８３】

ここでも、大きいしきい値及び傾斜条件の最大許容変化dSが、補助データの埋め込みの知覚性を低減して、データの種類によっては、埋め込みプロセスを完全に非知覚性のものにすることができる。傾斜条件の最大許容変化dSは、あらゆる値を有することができる。より大きい値により、より知覚されやすい歪みを伴うデータレートが得られ、より小さい値により、低いデータレートを伴う最小の歪みが得られる。16ビットオーディオでのdSに対する好適な設定は、ビット深さの大きさ2^bに等しい。ここでも、６ビット未満のビット深さで最小の歪みが生じるが、ノイズ及び攻撃に対してより強固にするために、より大きいビット深さを用いることができる。

【００８４】

しきい値2000（即ち66dB）及びビット深さ５を用いると、ＣＤ品質のオーディオ用には、データレートが40ビット/秒から100ビット/秒までの間、平均約75ビット/秒のデータレートが想定される。ビット深さ８では、ビットレートが平均100ビット/秒まで増加する。

【００８５】

変形例

以上では、特定の実施例について詳細に説明してきた。しかし、各利用のために、プロセスを最適化ずべく行うことができる簡単な変形が存在する。

【００８６】

一部のアプリケーションでは、非常に単純な実施例で、簡単なしきい値を用いて局所的マスキングの機会を特定し、そして、しきい値を超えた点、またはしきい値を超えた点の付近の他の点のＬＳＢに補助データを符号化する。こうした変形法は極めて単純であるが、従来法のＬＳＢ方式にくらべて低減された知覚性をもたらす。他の実施例では、値を変化させることが、検出基準に対する点を除去しないことを保証しなければならない。この場合には、単に、この変化がデータをしきい値の下にもっていくような箇所で埋め込みを省略することができ、そしてデータ点の現在値をしきい値に変化させて、復帰の段階でこのデータ点が飛ばされるようにすることができる。

【００８７】

攻撃またはノイズに対する強固さを増加させるために、次の変更を行うことができる。（攻撃は、原データの歪みを知覚させることなく、補助情報組込み済みの信号から補助情報を除去しようとする人物または機械として定義される。）

【００８８】

動的しきい値を用いて、補助情報の除去を困難にすることができる。動的しきい値の例が、オフセットした正弦波形である。動的しきい値を用いる際には、dSを小さく、2^bに近くして、プロセスが隣接点間差の分布を変化させないようにして、即ちこの分布は統計的に不可視であり、これにより攻撃者がこのデータを用いてしきい値を見出すことができない。

【００８９】

またdSが2^bより大きい際には、攻撃がＤＣシフトを用いる場合には、統計的ギャップを用いてしきい値を見出しうる。第２の好適実施例にとっては、第１実施例よりも、ＤＣシフトは明らかにより強力な攻撃であるが、しきい値は検出基準の一つに過ぎないので、第１の好適実施例にも影響がありうる。（耐攻撃の方法については、以下に考察する。）

【００９０】

ノイズに対する強固さをより良好にするために、プロセスはピーク及びしきい値交差について、より大域的な規定を用いることができる。特に、各側により多くの点が含まれるような、ピークまたはしきい値交差の規定を用いることができる。

【００９１】

最後に強固さを増加させるために、プロセスは補助情報において、いずれの種類のエラー訂正をも用いることができる。

【００９２】

データレートを増加させるために、次の変更を行うことができる。特に、ノイズに対する強固さが必要ない場合には、補助情報は、Ｎビットの語の間に特別な同期パルスを含める必要がない。これに加えて、負に向かうピーク及び／またはより多くのしきい値を用いて、ビットレートを増加させることができる。最後に、このプロセスは、より多くの情報を符号化するために、第２ビットの調整において、２進系以上のものを用いることができる。しかし、その結果はより知覚されやすいものとなるか、あるいは攻撃に対してより強固でなくなる。

【００９３】

好適な工夫は、正と負のピーク、及び／または種々のしきい値に、異なる補助情報を埋め込むことである。これに加えて、ステレオのファイルでは、各チャネルを別個に符号化することができ、あるいは符号化する点を左右のチャネル間で連続的に移動させて、符号化をチャネル間で移動させることができる。

【００９４】

知覚性を向上させうる変化は、補助情報の組込みにより、埋め込み点で値の大きな変化が生じる場合に、埋め込み点の後のデータ点を、埋め込み点の値に移すことである。

【００９５】

上述したように、データは時間に対するものである必要がない。例えば、データが振幅対周波数を表わすことができる。これに加えて、データは、特定の、周波数対時間の大きさとして見ることができる。増加したデータレートは、すべての周波数を含むことができる。換言すれば、スペクトルまたは分光において、埋

め込みを行うことができる。このプロセス及び対応する装置を使用するために、所定のデータのフォーマットを変更する必要がないことが有利である。

【００９６】

例えば、ＭＰＥＧ圧縮データのようなビットを低減したデータを考える。ＭＰＥＧ圧縮したデータは、スケールファクタ及び周波数係数を表現する一連のデータ点から構成される。例えば上述した２つの特定実施例のうちの１つを用いて、一連のＭＰＥＧデータ点中に補助データを埋め込むことができる。第１の特定実施例を用いる際には、特にスケールファクタを扱う際に、ピーク後の点を減少させて、ＭＰＥＧデータにおける量子化誤差が増加しないようにすることよりもむしろ、ピークを増加させるかあるいはピークのＬＳＢ（最上位ビット）を修正して、項が単に増加するようにしたい。ＭＰＥＧデータのような時間フレームに分割されるデータの使用において、データを埋め込むべき位置を決める際には、例えば連続するフレームからのスケールファクタまたは周波数係数、並びに１フレーム内のスケールファクタ及び異なる周波数の係数を表現するデータ点を用いることができることは当業者には明らかである。例えば、連続するフレームにおける特定周波数に対する係数を、一連の連続データ点と考えて、上述した実施例のうちの１つに従って、これらのデータ点を分析して、これらの連続点中にデータを埋め込むべき箇所を決めることができる。代替例では、１フレーム内のスケールファクタまたは異なる周波数に対する周波数係数を表現する一連のデータ点を、第１または第２の特定実施例に従って分析して、データを埋め込むべき箇所を決めることができる。

【００９７】

利用例

以下のことは、理解を助けるためのアルゴリズム例のいくつかの利用例に含まれる。このリストは完全なものではなく、開示した発明の有用性の重要例に過ぎない。さらに、以下に示す応用は、符号化の特定形態に頼るものではなく、ディジタル透かし、通信秘匿、またはデータ隠蔽の他の形態のも、代わりに用いることができる。

【００９８】

このプロセスは、著作権情報を埋め込むために用いることができる。この情報は、データがコピー可か否かを特定するための情報を含むことができる。ＣＤライター（書込み器）のようなコピー装置は、埋め込みデータを解読してコピーを阻止することができる廉価な集積回路を具えることができる。

【００９９】

これに加えて、作者または上演者の名前及び加入情報を埋め込むことができる。この利用法では、補助情報が小さく何回も反復され、各反復間に同期パルスを伴う。あるいはまた、実施例１を用いてコピー符号を埋め込み、実施例２を用いて作者の名前及び加入情報を埋め込む（即ち、いくつかの埋め込みデータを作品中に共存させる）ことができる。

【０１００】

こうした技術は、追加的情報を送るために用いることができる。この情報は、８ビット語のASCIIまたはANSI（３２ビットとして定義されるディジタル語に含まれるべきものではない）、及び所望すれば、これらの語の間の同期パルスで送信することができる。この情報は、個人的なメッセージ、歌の歌詞、または作品の記述とすることができる。歌詞については、このことはカラオケ装置、ＣＤプレーヤまたはＤＶＤプレーヤに対して有用である。

【０１０１】

ディジタル圧縮

データ隠蔽及びデータ圧縮（ダイナミックレンジではなくビットレートの低減）の主な問題は、データを隠蔽するプロセスが、圧縮（符号化及び復号化とも称される）として知られているディジタルビット低減技法と調和しない、ということである。データ隠蔽の目的がデータを最小限に知覚可能にすることであり、圧縮の目的が、知覚性が最小の部分を除去することなので、この不整合が生じる。

【０１０２】

この目的のために、図１０Ａ及び図１０Ｂに、データ隠蔽用のプロセスの例を示し、これは一部の点ではデータを圧縮しなければならない場合がある。このことは例えば、データを送信する間に発生しうる。

【０１０３】

図１０Ａでは、ボックス６００で示すように、上述したプロセスまたは他の何らかの方法を用いて補助情報を非圧縮データ中に埋め込む。次に、データを圧縮する必要がある際には、ボックス６１０に示すように、上述した方法または他のいずれかの方法または他の何らかの方法によって補助情報を復帰させる。圧縮及び非圧縮データにおけるデータ隠蔽用のアルゴリズムは、同じアルゴリズムとすることができ、異なる原データを用いることだけの違いである。あるいはこれらのアルゴリズムが異なってもよい。

【０１０４】

図１０Ｂでは、ボックス６２０に示すように、上述した方法または他の方法によって圧縮データから補助情報を復帰させて、このデータを伸長させて、補助情報を非圧縮データ中に埋め込んでいる。最後に、６３０に示すように、必要な際には、上述した方法または他の方法を用いて、補助情報をデータから復帰させることができる。ここでも、圧縮及び非圧縮データにおけるデータ隠蔽用のアルゴリズムは、異なる原データを用いることが違うだけの同じアルゴリズムとすることも、異なるアルゴリズムとすることもできる。

【０１０５】

上述したように、図２は、論理プロセッサ及び記憶装置１８によって実現できることを表わす。図１２に、ディジタルプロセッサ１２００及びディジタルメモリ１２１０での実現を示す。ディジタルプロセッサ１２００は、ディジタル信号プロセッサ（ＤＳＰ）、汎用中央処理装置（ＣＰＵ）、またはメディアプロセッサを含めた専用ＣＰＵと同等のものとして定義することができる。適切なＤＳＰチップは、テキサスインスツルメンツ社のTMS320の製品ラインナップのうちの１つである。ＣＰＵは、インテル社のPentium(登録商標)ラインナップまたはモトローラ/ＩＢＭ社のPowerPC製品ラインナップのうちの１つである。図５～図９の手続きの設計は、現在技術の状況に精通した者であれば直ちに行うことができる。

【０１０６】

これに加えて、図１３に示すように、現在技術の状況に精通した人ならば、このプロセスを、独立回路または特定用途向け集積回路（ＡＳＩＣ）のアナログま

たはディジタル回路で実現することができる。このアナログ及びディジタル回路は、次のデバイスのあらゆる組合わせを含むことができる：ディジタルーアナログ変換器（Ｄ/Ａ）、サンプルーホールド回路、遅延素子、アナログーディジタル変換器（Ａ/Ｄ）、及びプログラマブルロジックコントローラ（ＰＬＣ）。プログラマブルロジックアレイ（ＰＬＤ）も同様に用いることができる。現在技術の状況に精通した者は、図５～図９の記述及び手続きが与えられれば、容易に回路を設計することができる。

【０１０７】

図１１Ａ及び図１１Ｂに、論理プロセッサ及び記憶装置が通常、埋め込み装置７００及び復帰装置７７０を具えている様子を示す。埋め込み装置７００は次のものを具え、これらは、原データ７２０及び補助データ７３０を読むためのデータ読み取り器７１０、比較器７４０、即ちデータ点を既知の値または他のデータ点と比較するための回路または装置、及び補助データ組込み済みのデータ７６０を恒久記憶媒体または一時記憶媒体に書き込むための書込み器７５０である。

【０１０８】

復帰装置７７０は次のものを具えている。まず補助データを組み込んだデータを読み込むためのデータ読み取り器７１５であり、これらは埋め込み用のデータ読み取り器７１０と同一にすることができるが、異なるものとすることもできる。そして比較器７４５、即ちデータ点を既知の値または他のデータ点と比較するための回路または装置であり、必要ならば補助ビットを生成することができる。ここでも比較器７４５は埋め込み用の比較器７４０と同一にすることも、異ならせることもできる。補助情報はメモリから取り去ることができ、あるいはそれ相当の利用のみのために表示することができるので、データ書込み器は必ずしも必要ではない。

【０１０９】

発明の見通し

以上の記述より、補助情報を原データ中に隠蔽するための上述したプロセス及び装置が有効なものであり、知覚されにくい形のものであることは、読者にとって明らかであり、そしてこのプロセスをＣＤ品質のオーディオでテストすること

によって実証することができる。これらの利点は主に、信号を周波数領域に変換する必要なく、補助データを隠す箇所を見出すことによるものであり、このためマスキングにより、補助データの知覚をブロックまたは低減することができる。

【０１１０】

耐改ざん性及び耐攻撃性

上述したように、本明細書に詳述する本発明のさらなる要点は、に関するものである。埋め込みデータの改ざん及び攻撃に対する耐性を増加させることに関するものである。説明の都合上、ここでは「攻撃」という語を用いるが、埋め込みデータを故意に除去しようとする尽力、及びこうしたデータの偶発的な除去の両者を含めた意味である。攻撃には複写を含めることができ、これは、埋め込みデータを１つのセグメントから他のセグメントに複製または模造することができることとして定義される。攻撃には修正も含めることができ、これは埋め込みデータを、例えば「コピー不可」から「コピー可」にすることのように所望の形に変更することである。

【０１１１】

攻撃に対してより強固にした埋め込みデータを用いる方法、即ち許可及び登録プロセスを記述した２つの実施例について、以下に詳細に説明する。これに加えて、埋め込みデータの複写及び修正に対する強固さを向上させた実施例を、動的ロック及びロック解除を含めて開示する。

【０１１２】

第１の実施例は許可プロセスを利用するものであり、これは埋め込みデータを用いて、コピー、再生、または他の再現法のような動作を許可することである。このため、埋め込みデータが攻撃によって除去された場合には、原データが使いものにならなくなっているので、エンドユーザは何も得られなくなる。埋め込みデータが複写及び修正に対して強固である際には、このプロセスの改善がなされる。

【０１１３】

第２の実施例は登録プロセスを利用するものであり、ここでは記録装置が自分の登録情報をデータ中に埋め込む。本実施例では、記録装置とは、ＣＤまたはＤ

ＶＤ書込み器のような物理的装置、あるいはＭＰ３またはＡＡＣ符号化器のような仮想的装置のことを称しうる。この登録プロセスは、記録装置が購入時に登録されていることを仮定すれば、あらゆる違法メディアを元の所有者までたどることを可能にする。最後の最後に、違法メディアにより、特定記録装置の購入場所まで突き止めて、善良な開始点に対して法的強制力を与えるものである。

【０１１４】

動的ロック及びロック解除の実施例は、現在及び将来の埋め込みデータ技法の、複写及び／または修正に対する強固さを向上させるものである。動的ロックは、例えば次のステップの一方または両方を具えることによって、埋め込みデータをメディアに応じたものにする。第１ステップは、メディアによる補助情報の修正を含む。第２ステップは、できれば第１ステップで修正した補助情報の暗号化を含む。暗号化技法は、ＲＳＡ、ＤＥＳ、または他の適切なアルゴリズムとすることができる。補助情報を動的にロックした後に、これらを原データ中に埋め込む。動的ロックの各ステップが、独自の利点をもたらす。しかし、両ステップを含めると、修正したものでも創作したものでも、メディア間で転送不可能な補助情報が生成される。

【０１１５】

動的ロック解除プロセスは逆のステップを実行するものであり、動的ロックプロセスにおける各特定ステップを実行していることを仮定する。第１ステップは、復帰させたデータの暗号解読を含む。第２ステップは、第１ステップを実行したか否かに応じて、第１ステップの出力または復帰したデータを直接、修正取り消しして、これにより元の補助データを生成するものである。

【０１１６】

許可及び動的ロックのプロセス及び装置の５つの利用法について、ここで簡単に記述し、そしてプロセス及び装置の両者を理解する手助けとするために、以下で詳細に説明する。これらの利用法は、(1)依頼者の再生装置によってのみ再生可能なように、圧縮したメディアを配布すること、(2)埋め込みデータがあることを利用して、１回のみコピーのアクセスを指定すること、(3)ＤＶＤメディアの保護、(4)写真入りカードの確認、及び(5)保全した秘密メッセージの送付、を

含む。

【０１１７】

第１例の利用法では、ＭＰ３のソフトウエアプレーヤを有するコンピュータのようなメディアプレーヤをインターネットのサイトに接続して、ＭＰ３フォーマットの歌のようなメディアをダウンロードする。このプレーヤが固有の識別子をインターネットのサイトに送って、そこで原データを用いてこの識別子を修正し、その結果は暗号化されたものとなる。次に修正及び暗号化した識別子を原データ中に埋め込んで、識別子組込み済みの原データをプレーヤにダウンロードする。このメディアプレーヤは、識別子組込み済みのデータから識別子を抽出して、自分の識別子と比較することができる。これらの識別子が一致して、データ制限のような追加的な情報を確認した場合には、プレーヤがデータを再生する。識別子組込み済みのデータが、異なる識別子を有する第２のプレーヤにコピーされた場合には、この第２のプレーヤが識別子組込み済みのデータを再生することがない。

【０１１８】

無許可の人物が識別子を特定できた場合には、この人物がこの識別子を他の歌に埋め込んで、自分のプレーヤで再生することが可能になる。識別子を暗号化することによって、たとえ無許可の人物が識別子組込み済みのデータから補助データを抽出することが可能であっても、この人物が識別子を特定不可能になる。これに加えて、プロセスが元の情報で補助情報を修正することを含んでいない場合には、メディア間で埋め込みデータをコピーすることが可能である。最後に、暗号キーは適切な取扱いも必要であり、識別子はプレーヤ識別子以外の追加的な情報を含むことができる。

【０１１９】

第２例の利用法は、固有の識別子よりもむしろ、「allow no copying（コピー不可）」、「allow copying one time, but not copying of a copy（１回だけコピー可、再コピー不可）」、及び「allow unlimited copy（無制限コピー可）」のような所定のコピー符号を含むものである。レコーダがこのコピー符号を復帰させて、この符号によって許可されない限りコピーしない。コピーしたものに

は、「allow copying one time...」符号または「allow no copying」符号のいずれかを含めることができる。放送用には、プレーヤ及び放送装置が共に、符号を事前に知っているか（即ち所定の符号）、あるいはこの符号を含めて放送することができる。

【０１２０】

第３例の利用法は、２つの方法が望ましい。第１の方法は、原データ中に埋め込まれた所定の識別子を復帰させずに、ＤＶＤプレーヤＤＶＤを再生するものである。特別な安全性のために、中央データベースにあるキーまたはＤＶＤのコピー不可のセクション内のキーで識別子を暗号化することができる。第２の方法では、許可されているコピーの世代を識別子が制御することができ、これは識別子が存在しない場合には、コピーを作成することができないことに他ならない。あるいは、両方の種類のコピー管理用に２階層の識別子が存在しうる。

【０１２１】

第４例の利用法は、写真入りカードの画像内にソースデータを埋め込むことを含み、この画像は、運転免許証やクレジットカードのような認証目的に使用される写真のようなものである。写真入りカード読み取り器で復帰させた情報が中央データベースにある情報と一致しない場合には、このカードを偽造と認識して、使用を認可しない。なお、この情報及びキー交換は安全に伝送しなければならない。

【０１２２】

第５例の利用法は、メディア内に隠蔽した秘密情報を安全に伝送できるようにするものである。大部分の部外者は、秘密メッセージが添付されていることを知らない。添付を発見した場合でも、埋め込みデータがメディアに応じたものであり、かつ暗号化されていれば、隠し情報がなりすまし者によって読まれたり、修正されたり、及び／または他のメディアに転送されたりすることがありえない。埋め込みデータの所望の保護または認証を行うために、公開／秘密キーのような異なる種類の暗号化法をもちいることができる。この隠し情報は、受信側の人または機械が動作を実行することを可能にする。

【０１２３】

これらのプロセス用の好適な装置は、できればＤＳＰチップあるいはカスタムのアナログまたはディジタル回路を含む論理プロセッサ、及びメモリを含む。この開示が与えられ、かつ暗号化法及び電気技術の現在状況に精通していれば、この構成及び機械語は容易に設計することができる。

【０１２４】

前述したことの詳細な説明に戻る前に、いくつかの定義について考える。メディア及びコンテンツは、オーディオ、ビデオ、静止画像、これらの組合わせ、及び他の関連する形態を含むが、これらに限定されるものではない。メディア及びコンテンツという用語は互換的に用いる。メディアとは記憶媒体のことを称するものではない。メディアまたはコンテンツのセグメントは、歌、歌の一部、映画、映画の一部、サウンドトラックの一部または全部、静止画像の一部または全部、味覚、触覚、及び嗅覚を含むが、これらに限定されるものではない。原データとは、生の、保護されていないデータである。補助情報とは、原データ中に埋め込むべきあらゆるデータを称する。図２１のＩＤ１４０は補助情報のことを称し、プレーヤＩＤ、許可されたコピー回数、使用時間またはデータの制限、及び作者、著作権、出版元、歌の歌詞または詳細画像のようなコンテンツ拡張情報、のような情報を含むことができるが、これらに限定されるものではない。埋め込みデータとは、実際に原データ中に埋め込むデータのことである。埋め込みデータは、埋め込みプロセス中に使用する変換による補助データとは異なる。この変換は、動的ロックに含まれる修正プロセス及び／または暗号化、及びビット操作、パルス幅変調、あるいは周波数変換または擬似ランダムノイズ列での拡張のような埋め込みプロセスを含むことができる。埋め込みデータを原データに加えると、補助情報組込み済みのデータになる。攻撃に対する強固さは、埋め込みデータが提供または防止しようとすることを回避することとして定義される。最後に、海賊行為（著作権侵害）者とは、違法なデータの入手、及び保護された装置の使用を試みる者のことである。

【０１２５】

許可プロセス

図１４に、好適な許可プロセスを示す。このプロセスは、図２２に示すような

論理プロセッサ９００及びメモリ９１０を用いる。まずボックス１０に示すように、プロセッサ９００は補助データ組込み済みのデータ５から補助データを復帰させて、これをメモリ９１０に記憶する。次にボックス２０に示すように、プロセッサ９００は埋め込みデータが所望の動作を許可するものであるか否かを特定する。Yesであれば、ボックス３０に示すように所望の動作が許可される。Noであれば、ボックス４０に示すように所望の動作が不許可になる。

【０１２６】

登録プロセス

図１５に登録プロセスを示す。このプロセスは、固有の登録符号３０５を各記録装置３００に割り当てること、及びボックス３１０に示すように、記録の際に登録符号３０５をメディア内に埋め込むことを含む。次に、公開市場３２０において違法メディアを発見した際には、ボックス３３０に示すように、登録符号３０５によって、このメディアから記録装置の所有者を突き止めることができる。

【０１２７】

このプロセスは、購入時に記録装置を登録することを想定している点で、銃砲登録に類似している。最後の最後に、違法メディアから記録装置及びその購入場所を突き止めて、法的強制力を手助けすることができる。

【０１２８】

この記録装置は物理的装置とすることも仮想的装置とすることもできる。物理的装置は、ＣＤまたはＤＶＤ書込み器を含むことができる。仮想的装置は、ＭＰ３リッパーまたはＡＡＣ符号化器のような、プロセッサ９００及びメモリ９１０を用いてディジタル圧縮（ビットレートの低減）を行うソフトウエアプログラムを含むことができる。メディアとは知覚されるデータのことを称し、記憶媒体を称するものではないことに留意されたい。

【０１２９】

動的ロック

図１６に、動的ロックにより補助データの複写をブロックする方法を示す。コンテンツ間で埋め込みデータをビット対ビットでコピーすること、及び埋め込み情報を復帰させて、異なるコンテンツ中に再埋め込みすることの両者について、

複写をブロックして、この異なるコンテンツが認証済みとわかるようにする。

【０１３０】

特に、補助情報を修正さえすれば、海賊行為者が正確な修正取り消し方法及び埋め込みデータの再修正方法を発見せずに、埋め込みデータを１つのメディアのセグメントから他のメディアのセグメントに移動できなくなる。補助情報を暗号化さえすれば、海賊行為者が補助情報を入手できなくなる。海賊行為者は埋め込みデータを復旧させることはできるが、このデータが暗号化されているので、これを解読することはできない。両ステップ中には、補助情報を１つのメディアセグメントから他の新たなメディアセグメントに移動させることができない。補助情報を直接移動させると、復帰させたデータの修正取り消しを行うために用いる新たなメディアセグメント中の値が、原データ中のデータを修正した箇所の値に一致しないので、動的ロックの修正ステップにより、新たなメディア中の埋め込みデータの修正取り消しが不正確に行われる。海賊行為者が埋め込みデータの修正取り消し及び再修正を試みるならば（このステップの詳細は既知である）、データを新たなメディアセグメントに移動させるために、海賊行為者はまず、このデータを暗号解読するためのキーを持たなければならない。

【０１３１】

図１７に、排他的論理和（ＸＯＲ）関数用の入力及び出力を示す。ＸＯＲの逆もＸＯＲであり、極めて有効である。

【０１３２】

図１８Ａに、動的ロック及び埋め込みプロセスの概要を示す。プロセス全体は３つのステップを含むが、最初の２ステップのいずれか（または両方）、即ち動的ロックのステップを飛ばすことができる。しかし、動的ロックの両ステップを実行すれば、データの複写の困難さを向上させることができる。これに加えて、最後の２つのステップの順序を入れ替えることができる。通常、他のコンテンツを保護する理由で、埋め込みデータを含めたコンテンツを暗号化する際には、あるいは修正ステップが、キーの修正を必要としないことのように、いくつかの望ましい特徴を有する際には、この入れ替えが有益である。

【０１３３】

ボックス６００の１番目のステップでは、元のコンテンツ(c)にもとづいて、埋め込むべき補助データ(d)を修正する。このステップは、補助データを元のコンテンツに応じたものに修正して、コンテンツ間で埋め込みデータを、ビット対ビットでコピーできないようにすべく設計されている。コンテンツの選択したビットをコンテンツにとって制限的なものにして、コンテンツを認証済みに見せかけるために、新たなコンテンツ中でこれらのビットを変更できないようにすべきである。望ましい関数は排他的論理和（ＸＯＲ）演算子である、というのは、ＸＯＲの逆関数もＸＯＲであり、かつディジタルプロセッサ上で有効に実現できるからである。

【０１３４】

ボックス６１０の２番目のステップでは、修正したデータを暗号化して、埋め込みデータから元の補助ビットを得られないようにする。これにより、元の補助ビットを異なるコンテンツ中に再埋め込みして、この異なるコンテンツを認証済みに見せることができなくなる。補助データを暗号化する前に、元のコンテンツによって修正しない場合には、この補助データを元のコンテンツから新たなコンテンツに、ビット対ビットでコピーして、この新たなコンテンツを認証済みに見せることができる。ＤＥＳ及びＲＳＡを含めた、既存及び将来のあらゆる暗号化法を、既知のキー管理方法と共に用うることができ、これらの方法はすべて、従来法に良く記述されている。

【０１３５】

ボックス６２０の３番目のステップでは、暗号化及び修正した（動的にロックしたというラベルを付した）補助データを、元のコンテンツ中に埋め込む。

【０１３６】

図１８Ｂに、補助データを復帰させて動的にロック解除するために用いるプロセスの概要を示す。プロセス全体は３つのステップを含み、各ステップは、データを埋め込む際に対応するステップを実行している場合のみに実行すべきものである。これに加えて、埋め込み中に最後の２つのステップの順序を入れ替えている場合には、この復帰プロセス中に、これらの２つのステップに対応するステップを入れ替えるべきである。

【０１３７】

ボックス６３０の１番目のステップでは、コンテンツか埋め込みデータをら復帰させる。この時には、埋め込みデータが暗号化及び修正した補助データから構成される。（動的ロックのステップを実行していることを仮定する。）ボックス６４０の２番目のステップでは、復帰したデータを暗号解読する。ボックス６５０の３番目のステップでは、ステップ２の出力の修正取り消しを行う。その結果は元の補助データとなる。

【０１３８】

これに加えて、動的ロック及びロック解除には、関係データを用いることができる。関係データは、歌の歌詞または写真入り認証カードの人物の住所のような情報を含むことができる。

【０１３９】

図１９に、知覚されないように（即ち透かし）データを埋め込んだ際の、動的ロック及びロック解除の修正部分のいくつかの実現例を示す。図１９には修正部分のみを示してあるが、所望すれば、修正した補助情報を埋め込み前に暗号化して、復帰後に（ただし修正取り消しを行う前に）暗号解読することができる。これに加えて、補助情報の修正を飛ばすことができ、そして埋め込み前に補助情報の暗号化のみを行って、復帰後に暗号解読することができる。暗号化プロセスについては詳細に説明しない、というのは現在技術の状況に精通した者であれば、その実現方法は明らかであるからである。

【０１４０】

図１９Ａに、前述した装置に適用するような動的ロック及びロック解除を示す。動的ロックについては、ボックス２００のピーク値またはしきい値交差の値を排他的論理和（ＸＯＲ）の演算で用いて、次のＮ個の補助情報ビットを修正し、ここでＮは、データ中の１サンプル当たりのビット数である（例えばＣＤオーディオ用には１６ビット）。次に、局所的にマスクした差分Δのビット操作を用いて、補助情報のこれらの修正したＮビットを（例えば上述した方法によって、）随意に暗号化して埋め込む。修正した補助情報を全部埋め込むか、あるいは修正した補助情報を繰り返し埋め込みながら、原データを全部使い終わるまで、次の

Ｎ個のピークのグループ、等々について、このプロセスを繰り返す。

【０１４１】

上述したプロセスを用いて、埋め込みデータを復帰させ、（必要ならば）暗号解読し、そして修正取り消しを行うことができる。この修正取り消しプロセスは、修正プロセスの逆である。ＸＯＲ関数の逆もＸＯＲであるので、補助情報組込み済みのデータ及び暗号化した補助情報を、ＸＯＲ関数に適用する。ピーク値が原データのピーク値と同一であるということが重要である、というのは、これらは埋め込みプロセス中に変化しないからである。

【０１４２】

例えばＣＤオーディオを使用する際には、Ｎが１６である。このため、例えば補助情報の最初の１６ビットを、最初のピーク値によってＸＯＲを用いて修正する。次に、これらの修正した補助情報ビットを随意に暗号化して、現在のピーク及び次の１５個のピークの後の各データ点に埋め込む。データを全部埋め込むか、あるいは原データを全部使い終わるまで、次の１６個のピーク及び補助情報ビットのグループ、等について、このプロセスを繰り返す。全部のビットを埋め込み終わった後に、補助情報の最初の１６ビットについてこのプロセスを再開することによって、修正及び随意に暗号化した補助情報をデータ内に繰り返し埋め込むことができる。

【０１４３】

埋め込みデータを復帰させて、（暗号化してあれば）暗号解読して、ＸＯＲ演算の逆で修正取り消しを行うことができ、ＸＯＲ演算の逆もＸＯＲ演算である。これにより、復帰させ暗号解読した埋め込みデータ及び最初のピーク値とのＸＯＲ演算を実行することによって、補助情報の元の最初の１６ビットが得られる。補助情報を全部見出すか、あるいは補助情報組込み済みのデータを全部やり終えるまで、補助情報組込み済みのデータ及び埋め込みデータの１６個のピークの次のグループ、等について、復帰プロセスを継続する。

【０１４４】

埋め込みのための修正及び復帰のための修正取り消しの際には、補助情報中の１６ビットのグループの位置に適切に追随することが非常に重要である。

【０１４５】

上述した技法は、補助情報組込み済みのデータ中の同期パルスを可能にする。これらの同期パルスを用いて、補助情報の修正において用いた値に合わせて、補助情報を整列させることができる。例えば、補助情報を修正するために用いたピークの後にデータを埋め込むのではなく、同期パルスを埋め込んで、これを復帰プロセス中の整列用に用いることができる。

【０１４６】

図１９Ｂに、Aris Technologies社のJack Wolosewiczによる米国特許第5,774,452号"Apparatus and method for encoding and decoding information in audio signals"の発明）に適用される動的ロック及びロック解除を示し、これは参考文献として本明細書に含める。この場合については、ボックス２２０に示すように、パルス幅変調（ＰＷＭ）したビット流の埋め込みより時間的に先行して発生するデータ値を、補助情報と共にＸＯＲ演算で用いて、埋め込みデータの修正及び修正取り消しを行うことができる。この場合には、すべての補助情報を修正するために、いくつかの値を用いる必要がある。例えば、１６ビットデータを用いて256ビットの補助情報を埋め込む際には、動的ロック及びロック解除プロセスが先行する１６個の元のデータ点を用いて、すべての補助情報を修正する。データを埋め込んだのと同じ順序でデータを受け取る限りは、補助情報を修正するために用いたデータ値が先行する埋め込みビット流と重複しているか否かは問題にならない。このことが問題になるような構成が発見された場合には、２番目の埋め込みビット流を飛ばして、これに、補助データ組込み済みのデータ中で飛ばしたという目印を付けておくことによって、容易に取り扱うことができる。

【０１４７】

図１９Ｃに、擬似ランダムノイズ（ＰＮ）列にもとづいて、動的ロック及びロック解除を埋め込みデータに適用する方法の概要を示す。１つの実施例では、ボックス２５０及び２７０に示すように、ＰＮ列がＭ番目のデータ点を飛ばして、ここでＭは、データ（Ｎ）中の１サンプル当たりのビット数×各補助情報ビットに適用するＰＮ列セグメントのビット長に等しい。このＭ番目のデータ点を、ｂビットの補助情報と共にＸＯＲ演算で用いて、補助情報を修正することができる

。例えば、各補助情報ビットをＰＮ列の1024ビットのセグメントと共に１６ビットのオーディオに埋め込み、補助情報が６４ビット長であるものと仮定する。そうすれば、ＰＮ列を16384ビット（Ｍ＝1024ビットのＰＮセグメント×１６ビットのオーディオ）の原データに加えた後に、他の原データ点を飛ばして補助情報を修正する。各補助情報を埋め込むためには、これらのセグメントのうちの４つ（６４ビットの補助情報/１６ビットのオーディオ）が必要になる。これと等価なことで、65536個（1024ビットのＰＮセグメント×１６ビットのオーディオ×４つのＰＮセグメント）の原データ点毎に、隣接する４つの原データ点を飛ばして、修正した補助情報の全体を４つのＰＮセグメントの連続流中に埋め込むことができる。

【０１４８】

拡散スペクトル技術の現在状況では周知のように、修正して随意に暗号化したこの補助情報を用いて、ＰＮ列を原データに加える方法を制御することができる。特に、多くの応用では、修正した補助情報によってＰＮ列を位相シフトさせるか（即ち、０がＰＮ列の負の値を計って加算し、１が正の値を計って加算する。）、あるいは単に補助情報を乗算する。修正した補助情報を一旦復帰させたら、飛ばしたデータ点と共に逆ＸＯＲ演算を用いて、この情報の修正取り消しを行うことができる。

【０１４９】

ＰＮ列についての他の実施例は、飛ばしたデータ点を用いて、補助情報ではなく、ＰＮ列の次のＮビットを修正するものである。１つの点をスキップしている場合には、修正するＰＮビット数Ｍを、データ中のビット数Ｎに等しくすべきである。２つの点を飛ばしている場合には、Ｍが２×Ｎに等しい、等である。ＸＯＲ演算を用いてＰＮ列を修正して随意に暗号化することは、１つの方法に過ぎない。しかし、これによりＰＮ列のランダム性を低減して、他の修正関数を採用してランダム性を維持することができる。最後に、修正して随意に暗号化したＰＮ列をメディアデータ中に埋め込んで、これは埋め込みデータを復帰させるために用いられる。

【０１５０】

動的ロックの最後の実現方法では、ＰＮ列を用いる埋め込み方法に動的ロックを適用して、できれば原データを周波数領域に変換した後の原データ中に補助情報を置く箇所を特定する。こうした方法には、Dice社のMarc CoopermanとScott Moskowitzによる米国特許第5,613,004号及び第5,687,236号"Steganographic method and device"、及びAT&T研究所（Lacy J、Quackenbush SR、Reibman AR、Shur D、Synder JH(1998)）の特許出願中（詳細は欧州特許第889471号）の"On combining watermarking with perceptual coding"の方法が含まれ、これらは参考文献として本明細書に含める。これらの方法については、Ｎ個より多い連続埋め込みビットを決して有さず、そして非埋め込みビットから開始するために、データを埋め込むために用いたＰＮ列を必要としうるものであり、ここでもＮは原データ中の１サンプル当たりのビット数である。次に、最初の埋め込みビットに隣接及び先行する原データ点が、次のＮビットの補助情報を修正する。原データを全部埋め込んで、修正した補助情報が連続的に埋め込まれるようになるまで、このプロセスを繰り返すことができる。例えば、低周波数から高周波数までの周波数帯において、１６ビットのデータと３２ビットの補助情報で埋め込みを行う際には、最初の埋め込みビットの直下の周波数領域を用いて、次の１６個の補助データビットを修正する。次に、１７番目の埋め込みビットの直下の周波数帯における非埋め込みビットを用いて、次の１６個の補助情報ビットを修正する。次に、３３番目の埋め込みビットの直下の周波数帯における非埋め込みビットを用いて、最初の１６個の補助情報ビットを修正する、等である。

【０１５１】

同様の方法で、ＰＮ列を１つおき、あるいはｋ番目（ｋ＜Ｎであり、原データ中の１サンプル当たりＮビットである）のデータ点にＰＮ列を適用して、ＰＮ列に制限を適用する必要がないようにする。このプロセスは、Ｎ番目の埋め込みビットの次に非埋め込みビットがあることを保証するものであり、そして前述の方法と同様のやり方で実現することができる。

【０１５２】

ＰＮ列を用いたこれらの動的ロックの方法のすべてについて、動的ロック解除のプロセスはその逆であり、現在技術の状況に精通した人にとっては、以上の開

示より明らかである。

【０１５３】

図２０に、動的ロック及びロック解除を、コンテンツのデータ中ではなくヘッダ内に埋め込んだデータに適用することを示す。一般に、長さＬの補助データビットをロックして、コンテンツのフレームのヘッダ内に置いて、連続的に埋め込む。

【０１５４】

特に、図２０Ａのプロセスは、コンテンツのビットから開始し（ボックス７００）、そして補助データビットの先頭から開始する（ボックス７０５）。次に、Ｌ個の補助データビットをＬビットのコンテンツと共に、ＸＯＲまたは適用可能な関数を用いて修正し、そして／あるいは暗号化することによって（ボックス７３５）ロックする。これらＬ個のコンテンツのビットを、フォーマットとコンテンツのいずれかあるいは両方にとって制限的なものにして、これらのビットを異なるメディアのセグメント内に妨げなく複製できないようにすべきである。次に、Ｍビットのロックした補助データをフレームのヘッダ内に埋め込む（ボックス７１０）。これらのＭビットはＫ未満であるべきであり、ＬがＭで割り切れて、ＬビットをＬ/Ｍ個のフレームのヘッダ内に埋め込むことが好ましい。ＬがＭで割り切れない場合には、現在技術の状況に精通した人は余りを容易に取り扱うことができる。次にコンテンツをチェックして、まだフレームが存在するか否かを見極める（ボックス７１５）。コンテンツのフレームが残っていない場合には、プロセスを完了する（ボックス７３０）。コンテンツのフレームがまだある場合には、補助データをチェックして、前に修正したビットがあるか否かを見極める（ボックス７２０）。前に修正した補助ビットが残っている場合には、コンテンツの次のフレームを読み込んで（ボックス７２５）、ボックス７１０からプロセスを継続する。前に修正した補助ビットが残っていない場合には、コンテンツの次のフレームを読み込んで（ボックス７４０）、補助データをビット０から再開して（ボックス７０５）、ボックス７１０からプロセスを継続する。

【０１５５】

このプロセスは、補助情報が長さＬであることを仮定し、説明を容易にするた

めに、Ｌは適度に短いものとする。大多数の補助ビットを有する場合には、これらを長さＬのセグメントに分けて、毎回最初の補助ビットから開始するよりもむしろ、k番目のセグメントから開始することができることは明らかである。こうするために、補助ビットを長さＬのセグメントに分けて、各セグメントをＬ/Ｍ個のフレームのヘッダに埋め込むようにして、補助ビットをデータ内に埋め込む。

【０１５６】

攻撃に対する強固さを増加させるために、擬似ランダムノイズ（ＰＮ）のビット列を用いることができ、そして補助情報を修正するために、対応するＰＮビット値１を有する最初のＮ個の制限的なコンテンツのビットを用いることができる。

【０１５７】

あるいはまた、Ｍ個のロックした補助データビットを各フレーム内に埋め込む際に、Ｌ/Ｍ個のフレーム毎のＬビットよりもむしろ、各フレーム内のコンテンツの最初の重要なビットのみをＸＯＲ演算で用いることができる。この場合には、特に図２０Ａのボックス７２５及び７１０に示すように、各フレーム内で補助データビットを修正する。ここでも、ＰＮ列を用いて、元のオーディオのどのＭビットを用いるかをランダムに定めるようにする。Ｍを十分に大きくして、新たなコンテンツにおけるエラー訂正が、変更する必要のあるコンテンツのビットのすべてを修復して、補助データのビット対ビットの転送により、新たなコンテンツが認証済みに見えることを不可能にすることが重要である。Ｍの値はフレームの大きさ及び所望のビットレートに応じたものとする。

【０１５８】

それぞれＩＳＯ11172-3及びＩＳＯ13818-7であるＭＰＥＧ１及びＭＰＥＧ２仕様を含むＭＰＥＧデータのような、特にＭＰＥＧ２仕様に指定された階層III（ＭＰ３）またはＡＡＣオーディオのような、圧縮したコンテンツを用いる際には、フレーム及びヘッダのビットが所定のものであり、これらの仕様は参考文献として本明細書に含める。これにより、個人的、著作権、または付随的なビットを用いてデータを埋め込むことができる。生のＰＣＭオーディオ、データベース、

あるいはソフトウエアアプリケーションのような所定のフレームのないコンテンツを用いる際には、フレームを簡単に作成することができる。例えばコンテンツを、埋め込みデータ用のヘッダビットを有する1024ビットのフレームに任意に分割することができる。

【０１５９】

あるいはまた、ロックした補助データを、完結したファイル全体のヘッダとして規定されるグローバルヘッダ内のみに置くことができる。これら２つの場合は、ファイル全体を通してデータを埋め込むことよりも安全性が低い。ビットが多いほど、大きな力による攻撃に対してデータがより強固であることを意味する。放送のコンテンツについては、上述したようにコンテンツ全体を通してデータを埋め込んで、再生装置または人物が補助情報を受け取って、放送中の任意の時点応答できるようにすべきである。

【０１６０】

図２０Ｂに、図２０Ａで埋め込んだ補助データについての、復帰及び動的なロック解除プロセス用の擬似符号を示す。一般的に、連続的な方法で、コンテンツのフレームのヘッダから補助データを読み込んでこれらをロック解除することによって、補助データを復帰させる。

【０１６１】

特に図２０Ｂのプロセスは、コンテンツのから開始し（ボックス７５０）そして補助データビットの先頭から開始する（ボックス７５５）。次に、Ｎ個のコンテンツのビットを例えば図２２のメモリ９１０に蓄積して、次のＮ個の復帰させた補助データ（ボックス７８５）をロック解除するために使用できるようにする。次に、Ｍビットのロックした補助データをフレームのヘッダから読み込む（ボックス７６０）。次に、既存のフレームについてコンテンツをチェックする（ボックス７６５）。コンテンツのフレームが残っていない場合には、プロセスを完了する（ボックス７８０）。コンテンツのフレームが残っている場合には、補助データビットをチェックして、補助データビットが存在するか否かを見極める。補助ビットが残っている場合には、次のフレームを読み込んで（ボックス７７５）、ボックス７６０からプロセスを継続する。補助ビットが残っていない場合に

は、復帰させた補助データをロック解除して（ボックス７９０）、次のフレームを読み込み（ボックス７９５）、補助データをビット０から再開して（ボックス７５５）、コンテンツの他のＮ個のビットを蓄積し（ボックス７８５）、そしてボックス７６０からプロセスを継続する。

【０１６２】

例えば、復帰させた埋め込みデータをロック解除することは（ボックス７９０）、ボックス７８５で蓄積したコンテンツのＮ個のビットと、直前のＮ個の復帰させた埋め込みデータビットとのＸＯＲ演算（その逆もＸＯＲ）を実行すること、及び必要ならば暗号解読することを含む。これに加えて、各フレーム内にデータを連続的に埋め込んでいるで、復帰プロセスは、最後のビットを受け取った後に補助データビットどうしを重ね合わせて、これらの補助データビットがファイル全体を通して変化していないことを確かめなければならない（ボックス７９０）。ファイル全体中で補助データビットが変化している場合には、このファイルは認証済みのものではない。

【０１６３】

あるいはまた、他の修正関数を使用している場合には、その逆のものを使用すべきである。修正演算に使用したものと逆の演算では、復帰させた補助ビットと元のコンテンツのビットとで同じビットを用いることが重要である。フレームの最初のＭ個のオーディオビットを用いて補助データを修正する埋め込みの例については、フレームの最初のＭ個のオーディオビットを用いて、復帰させて暗号解読した、修正済みの補助データの修正取り消しを行うべきである。補助データを修正するためにＰＮ列を用いている場合には、データの修正取り消しを行うために同じＰＮ列を使用すべきである。

【０１６４】

代案の埋め込みステップを用いている場合には、これに従って補助ビットを復帰させる。例えば、グローバルヘッダ内またはリンクしたファイル内にビットを埋め込んでいる場合には、これらをそれぞれグローバルヘッダまたはリンクしたファイルから読み出す。

【０１６５】

最後に、補助データがＬより長いか、あるいはＬがＭで割り切れない場合には、適切なステップを踏むべきである。これらのステップは、動的ロック及びロック解除についての上述の説明が与えられれば、現在技術の状況に精通した人にとって明らかである。

【０１６６】

利用例

これら５つの利用例は、許可プロセス、及び動的ロック及びロック解除プロセスの理解の助けとするために記述するものである。これらの例の下にある総括的なプロセスは図２１に示すものであり、これに対応する装置は図２２及び図２３に示すものである。このプロセスは一般に、伝送装置１００で、ボックス１１０に示すようにＩＤ１４０を動的にロックすること、及びボックス１２０に示すように、ロックしたＩＤをメディア内に埋め込むことから始まる。本節の最初に規定したように、ＩＤとは識別子のことを称するが、あらゆる補助情報を含みうることに留意されたい。伝送装置１００は、符号化器、送信機、記憶媒体、等とすることができる。

【０１６７】

そしてメディアが受信装置１３０に伝送されて、受信装置１３０ではボックス１６０に示すようにロックされたＩＤを復帰させて、ボックス１７０に示すように動的にロック解除する。次に、ボックス１８０に示すように、復帰させたＩＤ１４０によって許可された場合には、適切な動作を可能にする。受信装置１３０は復号化器、プレーヤ、レコーダ、及び／または同様なものとすることができる。

【０１６８】

動的ロック及びロック解除のプロセスが暗号化及び暗号解読を含む際には、ボックス１５１、１５２、及び１５３に示すように、暗号キーをどこかに配置して安全に伝送しなければならない。暗号化法の現在技術状況に精通した者は、暗号キーの安全な伝送については十分理解している。キーの位置は、利用法の要求に依存する。５つの利用法には、種々のキー位置を示してある。大部分の利用法では、３つの可能な位置のうちの１つのみでキーが利用可能である。これに加えて

、暗号化及び暗号解読のキーは通常同一（対称）であり、以下の説明では暗号キーと称する。しかし、こうした状況の多くの場合に、公開／秘密キーでの暗号化も使用することができる。以下に、秘密／公開の暗号化を説明する際には、キーは公開暗号キーまたは秘密暗号キーとして指定する。最後に、所定の利用法では補助情報を伝送する必要がない、というのはこれらの値が予め規定されているからである。

【０１６９】

これに加えて、これらの利用法では、ＩＤ１４０の使用及び位置決め、及び伝送装置１００及び受信装置１３０の種類についても、より詳細に説明する。

【０１７０】

これら５つの利用例は、ＭＰ３データの配布、放送データへの１回コピーのアクセス、ＤＶＤのコピー保護、写真入りカードの証明、及び秘密データの伝送を含む。

【０１７１】

ＭＰ３データの配布に関しては、いくつかのシナリオを用いてその概念を説明する。これらすべてのシナリオが、ＰＣベースのソフトウエア及び携帯ＭＰ３のオーディオプレーヤ、及びインターネット経由の配布を共に含む。

【０１７２】

第１のシナリオでは、ＭＰ３データがインターネットに存在して、エンドユーザによって購入される。送達システムはエンドユーザのプレーヤと相互作用して、ボックス１５１に示すように、ＩＤ１４０及び暗号キーを、受信装置から伝送装置に安全に送信して、ＭＰ３データ中のＩＤ１４０を、暗号化を含めて動的にロックする。このシナリオでは、ボックス１５１に示すように、エンドユーザのプレーヤに暗号キーを置く。ＭＰ３ファイルを送達（即ちダウンロード）した後には、他のプレーヤは異なるＩＤを有するので、エンドユーザのプレーヤのみがデータを再生可能である。携帯及びＰＣベースのプレーヤがＩＤ１４０を共用することができ、このことはソフトウエアプログラム、及びＥＰＲＯＭまたはフラッシュメモリのような現在のディジタル電子回路によって容易に実現できる。ＩＤ１４０が動的にロックされているので、エンドユーザがＩＤ１４０を抽出して

、これを他の歌またはＭＰ３ファイルに使用することはできない。

【０１７３】

他のシナリオでは、ＭＰ３符号化器及びプレーヤをソフトウエアプログラムの一部とし、このプログラムは、ＣＤ、ＤＶＤ、または放送のオーディオを、暗号化を含めて動的にロックしたＩＤ１４０を含む埋め込みデータでＭＰ３オーディオに変換するものである。こうした例では、ボックス１５１に示すように、暗号キー及びＩＤ１４０を交換する必要がない。現在技術の状況では周知であるように、キー及びＩＤ１４０をエンドユーザから保護するように、ソフトウエアアプリケーションをプログラムすべきである。ここでも、ボックス１５１に示すキーをエンドユーザのプレーヤに置く。ここでも上述したように、ＭＰ３に変換したオーディオは、エンドユーザのシステム及び／または携帯プレーヤのみで再生可能であり、ＩＤ１４０を他の歌に移動することは不可能である。

【０１７４】

しかし他のシナリオでは、ボックス１５２に示すように、キーを中央データベース内に置くことができる。この構成は、プレーヤ及びＭＰ３オーディオのサンプル毎に異なるキーを可能にする。各歌毎に新たなキーを使用するので、この構成により、攻撃に対する強固さが増加するが、この構成は、特別な管理ツール及び責任を含むことになる。

【０１７５】

ＭＰ３オーディオについての最後のシナリオでは、オーディオの聴取に対する時間制限、あるいは超過するとオーディオを再生できなくなるような期限日を、ＩＤ１４０に含めることができる。プレーヤは、歌を再生した回数あるいは期限日が来たか否かを把握する。ＩＤ１４０は、歌を１台のプレーヤに限定しないデモ符号を含むことができる。

【０１７６】

１回コピーのアクセス（おそらくはタイムシフト（時間をずらした視聴）の目的で、メディアを１回だけコピーすることをエンドユーザに許可することとして規定される）に関しては、映画の放送についてこの概念を説明する。放送メディアでは、同一の暗号キーを全員が共有することが最良である。ボックス１５３に

示すように、キーを映画に埋め込んで放送し、放送毎にキーを変更することができる。これに加えて、埋め込みデータを暗号化していない場合にはキーが必要ではなく、このため伝送を簡略化することができる。最後に、１回コピーのＩＤ１４０を予め規定することができ、このことは、図２１に示すように、送信及び受信装置内でＩＤが既に規定されており、送信装置内ではＩＤ１４０を随意の位置に置くことを意味する。一旦放送を受信すると、復帰させたＩＤ１４０がデータを記録可能にして、レコーダが映画を記録して、１回コピーのＩＤ１４０を除去するか、あるいはＩＤ１４０を、メディアが１回コピーされていることを他のレコーダに知らせる所定の符号に変更することのいずれかができるようになる。

【０１７７】

ＤＶＤのコピー保護に関しては、２つのシナリオがある。第１のシナリオでは、埋め込みＩＤが動作を許可しない限りプレーヤがメディアを再生することができない。ボックス１５３に示すように、暗号キーは、ＤＶＤ上のコピー不可のアクセス位置に含まれる。プレーヤが正規のＩＤを復帰させずにＤＶＤデータを再生することができないので、このことは、ＤＶＤのディスクが存在する際のみに、ユーザがメディアを再生できることを意味する。埋め込みデータを暗号解読するためのキーが発見されず、それなしではプレーヤが動作しないので、ＤＶＤ全体のコピー（暗号キーはコピー不可なので、これを差し引いたもの）、あるいはコンテンツのファイルのコピーは不可能である。

【０１７８】

これに加えて、ボックス１５２に示すように、キーを集中的にアクセス可能なデータベース内に置いて、要求をしたエンドユーザのプレーヤにできるだけリンクさせる（結び付ける）。キーへのアクセスを監視するので、この構成により、攻撃に対する強固さが増加するが、この構成には、コンテンツの提供者及びに対する特別な管理責任及びエンドユーザに対する追加時間を含めることになる。Paul Schneck氏に与えられた米国特許第5,933,498号（参考文献として本明細書に含める）に記載のように、キーを購入して、自分のプレーヤ内のキーによって暗号化することもできる。ここでも、ＩＤ１４０を予め規定して、伝送装置１００内に存在させることができる。

【０１７９】

異なるシナリオでは、シリアルコピーマネージメントとして知られているように、所定のＩＤ１４０を用いて、レコーダを動作可能にして、所定数のコピーの世代を、または原本のみのコピーを許可することができる。ＤＶＤを録画する毎に、許可する録画世代が１つ少なくなるように、ＩＤ１４０を修正することができる。これは、できれば、録画世代及び元々許可された回数の記録を残すことによるか、あるいは許可された回数を低減することによる。シリアルコピーマネージメント用には、第２世代のＤＶＤでは透かしを除去することができる。この方法では、透かしが存在しない場合には、コピーを作成することができないことに留意されたい。最後に、両方の種類のコピー管理に対して２層のＩＤ１４０がありうる。

【０１８０】

写真入りカードの利用例は、ＩＤ１４０を埋め込んだ写真入りカードに画像を有することを含む。正規の情報が存在しない場合には、このカードは偽造であり、使用が認可されたものではない。動的ロック及びロック解除を適用した方法の安全性を増加させるために、写真あるいはこれに対応する氏名または住所のような関連データによってＩＤ１４０を可逆的に修正し暗号化して、カード間で、あるいは正規のカードから違法カードに情報をコピーできないようにする。合致するＩＤ１４０と暗号キーを、あらゆる伝送装置によってアクセス可能なデータベースのみに（即ち、伝送装置内に）記憶して、例えばＲＳＡキー交換または暗号化の現在技術状況では既知の他のいずれかの方法を用いて、このデータベースと写真入りカード読み取り装置との間で安全に伝送することができる。他の暗号化技術と同様に安全であること以外に、このプロセスの他の利点は、短いＩＤ１４０及び暗号キーを含めて、最小限のデータの伝送を必要とするということである。

【０１８１】

最後の利用例は、メディア内に隠蔽したＩＤ１４０内の秘密情報の安全な伝送を可能にするものである。大部分の部外者は、秘密メッセージが添付されていることを知らない。一旦受信装置が隠しメッセージを抽出すると、この受信装置、

これに接続した装置、あるいは人間が、ＩＤ１４０に含まれる隠し情報によって動作可能になる。隠し情報を見出した場合には、この隠し情報を、他のメディアのセグメントに移動すること、及び／または動的ロックを暗号化方法と共に用いることによって解明することから保護することができる。例えば、秘密情報を公開キーで暗号化している場合には、本人だけがこれを復元することができる。あるいはある人秘密キーで暗号化している場合には、その人の公開キーを用いてこのメッセージを受信する人または装置のみが、このメッセージがその人によって署名され、認証済みであることを知る。このメッセージを対称キーで暗号化している場合には、キーの保持者のみがこのメッセージを作成し、読み得たことになる。最後に、動的ロックの修正ステップを用いている場合には、異なるメディアのセグメントからメッセージが転送されたことを受信機が知る

【０１８２】

装置

図２２に、許可、登録、及び動的ロックのプロセスを実現するために用いることができる好適な装置を示す。このハードウエアは、論理プロセッサ９００及びメモリ９１０を含む。論理プロセッサ９００は、ディジタル信号プロセッサ（ＤＳＰ）、汎用中央処理装置（ＣＰＵ）、または特化したＡＳＩＣチップと同等のものとして規定することができる。適切なＤＳＰチップは、テキサスインスツルメンツ社のTMS320製品ラインナップのうちの１つである。ＣＰＵは、インテル社のPentium(登録商標)ラインナップまたはモトローラ/ＩＢＭ社のPowerPC製品ラインナップを含むことができる。現在技術の状況に精通した者であれば、これらのプロセスについての記述が与えられれば、直ちに設計を行うことができる。メモリ９１０は、いずれの種類のメモリも含む。

【０１８３】

図２３に、動的ロック用の装置の詳細を示す。特に、論理プロセッサ９００及びメモリ９１０が協働して、修正器１０１０及び暗号化器１０４０として動作しなければならない。修正器１０１０は、動的ロックの修正ステップを実行する。暗号化器１０４０は、動的ロックの暗号化ステップを実行する。

【０１８４】

図２４に、動的ロック解除用の装置を詳細に示す。特に、論理プロセッサ９００及びメモリ９１０が協働して、暗号解読器１０４５及び修正取り消し器１０１５として動作しなければならない。暗号解読器１０４５は、動的ロック解除の暗号解読ステップを実行する。修正取り消し器１０１５は、動的ロック解除の修正取り消しステップを実行する。動的ロック解除の修正取り消し器１０１５及び暗号解読器１０４５は、動的ロックの修正器１０１０及び暗号化器１０４０と同一または異なる回路を用いることができる。しかし、同一回路を用いる際には、動的ロック及びロック解除プロセスが異なる制御プログラムを使用する。

【０１８５】

拘束及びＩＤ割り当て

上述したように、本明細書に詳述した本発明の要点はメディア拘束と称するものであり、これは例えば海賊行為を制御しつつ、保護されたコンテンツに消費者が合法的にアクセスする方法である。基本的な概念は、コンテンツを特定のユーザまたは放送に対してロックして、再生装置が、現在及び前のＩＤ及び規則にもとづいてコンテンツをアクセス可能か否かを自動的に特定するようなＩＤを、コンテンツが含んでいるということである。こうした技術により、コンテンツの提供者にとっては、コンテンツの売上が増加することになりうる。

【０１８６】

本発明の１つの要点は、受信装置が、現在アクセスしているコンテンツ及び前にアクセスしたコンテンツの両者のＩＤの記録を取っておくことにある。このことは、再生装置が、新たなコンテンツのＩＤ、（コンテンツの提供者によって）コンテンツに設けられた規則、及び／または装置内の規則、及び装置によって以前に再生したコンテンツからのＩＤもとづいて、新たなコンテンツへのアクセスを制御することを可能にする。

【０１８７】

このＩＤはユーザまたは放送にリンクすることができる。ユーザＩＤは、ユーザが継続使用するために販売されたコンテンツに対して良好に作用し、放送ＩＤは、ユーザが放送から記録したコンテンツに対して良好に作用する。

【０１８８】

実現例は次の通りである。ユーザにリンクしたコンテンツについては、できれば各ユーザＩＤを有するコンテンツを既にアクセスした回数に影響されるような一定時間長だけアクセス可能であり、異なったユーザＩＤを有するコンテンツのトラック数を制限する制約を、再生装置が具えている。放送のコンテンツについては、放送ＩＤ及び随意に具えている規則を用いて、各放送の再生またはコピーを制限することができる。換言すれば、放送ＩＤについては、前記制限は、日付またはＩＤを再生した回数にもとづくものであり、放送ＩＤの総数にもとづくものではない。

【０１８９】

より詳細には。携帯ＭＰ３プレーヤが各歌のユーザＩＤの記録を取っておいて、前に再生した歌がＮ個の異なるユーザＩＤを含む場合には、旧ユーザＩＤの日付及びそのＩＤで歌を再生した回数により、旧ユーザＩＤを新しいものに置き換え可能か否かをプレーヤが決定することができる。同様に、放送ＩＤがメモリに含まれている場合には、ＭＰ３プレーヤが、ユーザがオーディオを、放送によってＹ回許可されているところをＸ回再生したこと、あるいは、放送が許可した使用期日が経過したことを注視する。

【０１９０】

こうするために、ユーザがＩＤカードを保有する必要がないので、ユーザにとっては装置の使用が容易である。これに加えて、グローバルデータベースがユーザをＩＤにリンクする（結び付ける）必要がなく、このためユーザがプライバシーについて譲歩することがない。例えば、ユーザが自分のＩＤを喪失した場合には、前のコンテンツからＩＤを得ることができる。しかし、ユーザＩＤまたは放送ＩＤを秘匿しておいて、他のプライバシーについての方法を用いることができる。コンテンツの提供者が望むようにメディアへのアクセスを制限するが、ユーザの不都合にならないことが最も重要である。

【０１９１】

ここでも、関連用語の吟味を順番に行う。再生装置とは、データ上の動作と同じことを、演奏、視聴、記録、あるいは実行可能な装置のことである。再生装置は、画像、オーディオ、ビデオを含むがこれらに限定されない、あらゆる種類の

受信データを提供することができる。再生装置が、ＭＰ３プレーヤにあるような携帯部分を有する場合には、コンテンツを携帯部分に載せる（ロードする）ローダを再生装置の一部分として考える。ＩＤは、ユーザＩＤまたは放送ＩＤとすることができる。例えば、多くのＭＰ３プレーヤは放送を録音することもでき、これらの放送は将来、できればディジタル放送に伴う透かしまたはヘッダのデータとして、埋め込み放送ＩＤを含む。コンテンツとは、所望するオーディオ、ビデオ、画像、または関連する他の受信データである。コンテンツ提供者とは、レコードのレーベル（商標権者）、映画スタジオ、及び独立アーティストを含むがこれらに限定されない。ヘッダファイル内のビットまたは透かしのように、コンテンツ内にＩＤを埋め込むか、あるいはコンテンツの暗号化及び暗号解読にＩＤをリンクさせることができる。最後に、メディア拘束のような他の方法に関連して、この自動ＩＤ管理を用いることができる。

【０１９２】

図２５に、自動ＩＤ管理プロセスの概要を示す。このプロセスでは、再生装置１００が、コンテンツ内に含まれるＩＤについて、前にアクセスされたことの記録を取っておく（ボックス１１０）。規則１２０を装置のハードウエア内に設けるか、かつ／あるいはコンテンツに含める。規則１２０は、コンテンツのＩＤにもとづいて、装置が新たなコンテンツをアクセス可能か否かを決定する。

【０１９３】

再生装置が、ＭＰ３プレーヤような携帯部分を有する場合には、再生装置の一部分として上述で規定したローダを用いて、携帯部分内に必要なメモリの量を低減することができ、これによりコストを低減することができる。このことは、携帯再生装置では、携帯部分に、この自動ＩＤ管理を実行するのに必要なすべてのメモリ及び処理ハードウエア（以下で詳細に説明する）を含めるか、あるいはローダと携帯部分との間でハードウエアを分割することができることを意味する。例えば、コンピュータがソフトウエアローダを用いて、ＭＰ３ファイルを携帯ＭＰ３プレーヤに載せる際には、このローダがコンピュータ上のＩＤについてのすべての情報を記憶することができ、再生装置がする必要があることは、各歌を再生した回数を数えて、コンテンツの最新リスト用の日付情報を維持することだけ

である。

【０１９４】

図２６に、前記プロセスの例を実現するための擬似符号を示す。この例では、規則１２０は、コンテンツ提供者の指定通りにコンテンツ内に含まれる制約２４５、並びに再生装置のハードウエアに含まれるデフォルト規則を含む。制約２４５は、コンテンツ２００から復帰される（ボックス２４０）。制約２４５は、設定した期間中に装置がアクセス可能な、異なるＩＤを有するコンテンツのトラック数を制限することができる。制約２４５は、特定ＩＤでコンテンツをアクセスした回数に応じて、ＩＤを記憶する期間を変更することもできる。制約２４５をコンテンツ内に埋め込むか、あるいはヘッダ情報またはリンクファイルとして添付することができる。

【０１９５】

使用の容易さのために、これらの制約を歌毎に変化させない方が良い、というのはユーザを混乱させうるからである。この制約は合意されたものであり、再生装置内に設定されていることが理想である。しかし、コンテンツ内に規則を含めることも実行可能な選択肢である。

【０１９６】

この好適なプロセスの詳細をさらに説明する前に、自動ＩＤ管理プロセスを実現するための装置例（図２７）を理解しておくことが重要である。このハードウエアは、論理プロセッサ３００及びメモリ３１０を含む。論理プロセッサ３００は、ディジタル信号プロセッサ（ＤＳＰ）、汎用中央処理装置（ＣＰＵ）、またはメディアプロセッサを含む特化したＣＰＵと同等のものとして規定することができる。ここでも、適切なＤＳＰチップはテキサスインスツルメンツ社のTMS320製品ラインナップのうちの１つである。ＣＰＵは、インテル社のPentium(登録商標)製品ラインナップまたはモトローラ/ＩＢＭ社のPowerPC製品ラインナップのうちの１つを含むことができる。論理プロセッサ３００を制御するためのコードの設計は、以上の擬似符号及び記述が与えられれば、現在技術の状況に精通した者にとっては簡単である。

【０１９７】

これに加えて、現在技術の状況に精通した人は、アナログ及びディジタル回路を用いて、独立回路または特定用途向け集積回路（ＡＳＩＣ）のいずれかの形で、論理プロセッサ３００を実現することができる。このアナログ及びディジタル回路は、次のデバイスのあらゆる組合わせを含むことができる：ディジタルーアナログ変換器（D/A）、比較器、サンプルーホールド回路、遅延素子、アナログーディジタル変換器（A/D）、及びプログラマブルロジックコントローラ（ＰＬＣ）。プログラマブルロジックアレイ（ＰＬＤ）も同様に用いることができる。

【０１９８】

メモリ３１０は、ＩＤ、最終再生日、及び各ＩＤでコンテンツをアクセスした回数のように、規則１２０が必要とする情報を記憶する。メモリ３１０は、標準的なコンピュータのランダムアクセスメモリ（ＲＡＭ）で構成することができる。再生装置の電源なしでも、メモリ３１０が前記情報を維持する場合には、これらに限定されないがおそらくは、充電可能なバックアップ電源と共にＲＯＭを用いるか、あるいはＥＰＲＯＭのように電源なしでも安定なメモリを用いることも望ましい。上述したように、携帯部分及びローダを用いる際には、メモリ３１０を２つの別個のモジュールから構成することができる。

【０１９９】

ここで、プロセスの例の詳細な説明に戻る。このプロセスは、装置１００が新たなコンテンツ２００を受け取ることから始まる。コンテンツ２００からＩＤ２１０を復帰させる。ＩＤ２１０をチェックして、これがユーザＩＤであるか放送ＩＤであるかを見極める（ボックス２１５）。

【０２００】

ユーザＩＤについては、次のことを行う。ＩＤ２１０が装置１００のメモリ３１０に既に存在する場合には（ボックス２２０）、再生回数及び最終アクセス日を更新して（ボックス２２２）、コンテンツを再生する（ボックス２３０）。ＩＤ２１０がメモリ３１０に存在しない場合には（ボックス２２０）、規則１２０をチェックする。他のＩＤがメモリ３１０に存在しうる場合には（ボックス２５０）、ＩＤ２１０及び現在の日付をメモリ３１０に追加して（ボックス２６０）

コンテンツを再生する（ボックス２３０）。他のＩＤを追加できない場合には、規則１２０をチェックして、既存のＩＤのいずれかが、古すぎるために置き換え可能であるか否かを見極める（ボックス２７０）。いずれかのＩＤが置き換え可能である場合には、古いＩＤをＩＤ２１０で置き換えて（ボックス２８０）、コンテンツを再生する（ボックス２３０）。置き換え可能なＩＤがない場合には、ユーザに警告を発して、コンテンツ２００へのアクセスを拒否または制限する（ボックス２９０）。このコンテンツを購入するための連絡先をユーザに提示することもできる（ボックス２９０）。

【０２０１】

より詳細には、規則によって装置が１０個のＩＤを記憶できるようにすることができ、そしてＩＤを一週間アクセスしていない場合には、これらのＩＤを置き換えることができる。

【０２０２】

これに加えて、ＩＤを再生した回数を用いて、古いＩＤを新しいものに置き換えるべきか否かを決定する（ボックス２７０）。この回数値はＩＤをメモリ３１０に保持する期間に影響しうるものであり、これにより、記憶しているＩＤが、ＩＤ２１０に置き換わることができる（ボックス２７０及び２８０）。例えば、記憶しているＩＤに関連するコンテンツを一週間アクセスしていない場合には、このＩＤを置き換えることができる。逆に、記憶しているＩＤに関連するコンテンツを少なくとも７回再生している場合には、このＩＤを最終アクセスから少なくとも１ヶ月保持すべきである。

【０２０３】

コンテンツ提供者の特定の必要に合うように設計することができる簡単な規則が、他に多く存在する。一部のものは差分式を用いて、ＩＤを置き換え可能か否かを決定するものである。例えば、ＩＤ用の回数を１日毎に１つずつ減らし、かつこのＩＤを含むコンテンツの再生毎に１つずつ増やして、この回数が０またはそれ未満になるか、あるいは最終アクセスの日付が一週間以上前である場合には、このＩＤを置き換えることができる。

【０２０４】

放送ＩＤについては、次のことを行う。ＩＤ２１０を検査して、このＩＤが既にメモリ３１０に存在するか否かを見極める（ボックス２５５）。存在しない場合には、ＩＤ２１０及び現在の日付を再生装置のメモリ３１０に追加して（ボックス２６５）、コンテンツを再生する（ボックス２３０）。ＩＤ２１０がメモリに存在する場合には、再生回数、記録日、及び／または最終アクセス日をチェックして、このコンテンツが再生可能であるか否かを見極める（ボックス２７５）。放送が２回の再生のみか、または一週間の再生か、あるいは特定日までの再生を許可することができる。放送の再生が許可された場合には、前記回数及び最終アクセス日を更新して（ボックス２８５）、コンテンツにアクセスする（ボックス２３０）。放送の再生が許可されなかった場合には、アクセスが制限されたことをユーザに通知して、該当するものがあれば、放送を購入するための連絡先または同様のコンテンツを提供することができる（ボックス２９５）。

【０２０５】

これに加えて、この装置は、ＩＤ、日付、及び回数のような情報のすべてをリセットするためのある方法を有するべきである。リセット機能は擬似乱数（ランダム）であるパスワード符号を必要としうるものであり、このためユーザは、装置をリセットするために、サポート（支援）に連絡する必要がある。例えば、パスワードは年月に応じたものであり、自動システムから得られる。リセットボタンは現在のすべてのコンテンツ並びにＩＤ情報をを消去する。これにより、人々がパーティで１台の携帯プレーヤを多くの友人と共に使用できるようになるが、コンテンツの消失により、海賊行為がやりにくくなる、というのは海賊行為が煩雑だからである。

【０２０６】

図２８に、前述した擬似符号を実現する前述の装置を含む携帯ＭＰ３プレーヤを示す。この場合には、論理プロセッサ３００を独立したプロセッサとするか、あるいはオーディオを伸長するプロセッサのアクセスを共用することができる。この装置は、できればプレーヤ４００の電源がない際にも、ＩＤ、データ、及び回数のような必要な情報を記憶するのに必要なメモリ３１０も含む。この装置は、このメモリをソフトウエアのローダと共用することができる。

【０２０７】

最後に、あらゆる再生装置において、論理プロセッサ３００を独立したプロセッサとするか、あるいは、ディジタル圧縮または伸長のように、この装置用のコンテンツを扱うプロセッサを時分割使用することができる。

【０２０８】

多重透かし

唯一の透かしの代わりに多数の透かしを用いることにより、種々の利点が生まれる。好適なシステムでは、１つの透かしが強固なものであり、メディアを保護することを宣言している。メディアをＭＰ３のような所望のフォーマットに符号化する際に透かしを埋め込む。このことは、透かしを追加することの強さは問題にはならないことを意味する、というのは、透かしをオーディオに１回追加して、配布者がオーディオと共にコピーしたに過ぎないからである。

【０２０９】

他の透かしは、メディアを再生及び記録することが可であると宣言するものである。この透かしは有効なものであり、透かしを除去しても利点が生じないので、透かしの除去を困難にする必要がない。例えばインターネット上でのダウンロードのように、メディアをユーザ、プレーヤ、レコーダ、及び／または記憶装置にリンクするためにオーディオを複製する度にこの透かしを埋め込まなければならないので、この透かしの有効性は望ましいものである。これにより、配布者にとってはコピー管理のコストが大幅に低減されることになる。これに加えて、プレーヤは通常、この有効な透かしを見出さなければならないだけなので、プレーヤのコストが低減されることになる。透かしが存在しない場合だけは、強固であるが演算密度の高い透かしでオーディオが保護されているか否かを、プレーヤが特定する必要がある。

【０２１０】

保護なしのメディアはいずれの透かしも含みえず、あらゆる装置によってあらゆる記憶装置から再生可能であることが最も重要である。

【０２１１】

より詳細には、図２９に、２つの透かしを採用するプロセスを示す。メディア

１００は不安全なフォーマットであり、このことは、メディア１００がいかなるコピー保護及び／または認証の透かしを含んでいなくても、装置がメディア１００を再生可能であることを意味する。ＭＰ３のようなフォーマットは、一部の作者が自分のコンテンツを無償で配布するために望むフォーマットである。しかし、自分たちのメディアが無償でコピー及び再配布されることを許可しておらず、自分たちのメディアを同じフォーマットで配布することを希望しないことに関心のある団体が存在する。

【０２１２】

透かし１１０は、メディアが保護されていることを宣言するものである。透かし１１０は除去することが極めて困難でなければならず、そして計算密度を高くすることができる。多くの既存の透かし法が以上の記述を満足し、将来にも透かし法が必ず設計される。

【０２１３】

透かし１２０は、メディアをユーザ、プレーヤ、レコーダ、及び／または記憶装置にリンクするものである。このリンクは、ユーザがこのメディアをコピー及び／または再生することができるか否かを特定する。透かし１２０は模倣されにくく、かつ計算効率の高いものでなければならない。

【０２１４】

図２９及び図３０に示すように、複製プロセス中に両方の透かしを特定回数だけ埋め込む。オーディオを符号化する際に透かし１１０を埋め込み、配布の際にオーディオと共にコピーする。これにより、透かしを追加することの計算密度はそれほど重要なものではなくなる。例えばメディアを配布する際、恒久記憶装置に置く際、あるいは個人用の符号化装置によって代替の形式から符号化する際のように、メディアを複製する際に透かし１２０を埋め込む。複製するとは、メディアを合法的に変換または配布することであり、コピーするとは、合法または違法な利用のために、メディアを正確にビット対ビットで、個別に複製することである。メディアを複製する度に透かし１２０を埋め込むので、その効率がコストの低減を生み出す。透かし１１０の後で透かし１２０を埋め込むので、透かしを階層化することが可能であり、このことは既存の技術で可能であることが知られ

ている。

【０２１５】

図２９及び図３１に示すように、随意的に、透かしを特定順序で探索及び復帰させる。まず、メディア上で透かし１２０を探索する（ボックス３００）。透かし１２０を復帰させたならば（ボックス３１０）、埋め込み情報を評価する（ボックス３２０）。埋め込み情報が正規のものである場合には、所望の動作を可能にする（ボックス３３０）。あるいはまた、埋め込み情報が正規のものではない場合には、所望の動作を不可能にする（ボックス３４０）。透かし１２０が発見されなかった場合に限って、メディア上で演算密度の高い透かし１１０を探索する（ボックス３５０）。メディアが保護されていることを透かし１１０が宣言している場合には、所望の動作を不可能にする（ボックス３４０）。透かし１２０が存在しない（か、あるいはメディアが扱い自由であることを宣言している）場合には、所望の動作を許可する。

【０２１６】

直前に詳述したプロセスを、メディアのコピー及び／または再生を制限するために用いることができる。

図３２に、本発明を実現するために使用しうるハードウエア装置を示す。このハードウエアは、論理プロセッサ４００及び記憶装置４１０を具えている。論理プロセッサ４００は、ディジタル信号プロセッサ（ＤＳＰ）、汎用中央処理装置（ＣＰＵ）、あるいはメディアプロセッサを含む特化したＣＰＵと同等のものとすることができる。適切なＤＳＰチップは、テキサスインスツルメンツ社のTMS320製品ラインナップのうちの１つである。ＣＰＵは、インテル社のPentium(登録商標)ラインナップまたはモトローラ/ＩＢＭ社のPowerPC製品ラインナップを含むことができる。現在技術の状況に精通した者にとっては、上述した手続きおよび説明が与えられれば、設計は簡単である。ディジタルプロセッサを使用する際には、記憶装置４１０がＲＡＭを含む。

【０２１７】

あるいはまた、現在技術の状況に精通した人は、このプロセスをアナログ及びディジタル回路で実現することができ、これらは独立回路または特定用途向け集

積回路（ＡＳＩＣ）のいずれかの形である。これらのアナログ及びディジタル回路は、次のデバイスのあらゆる組み合わせを含むことができる：ディジタルーアナログ変換器（D/A）、比較器、サンプルーホールド回路、遅延素子、アナログーディジタル変換器（A/D）、及びプログラマブルロジックコントローラ（ＰＬＣ）。プログラマブルロジックアレイ（ＰＬＤ）も同様に用いることができる。

【０２１８】

コンテンツのスクランブル

上述したように、コンテンツの信号をスクランブルすることが往々にして望ましい。次の説明はこうしたスクランブル技術の改良について吟味するものである。

【０２１９】

こうしたスクランブル技法の１つに、元のディジタルデータ全体を通して検出基準を探索し、そして、検出基準の位置に影響しないようにする既知の方法か、あるいは検出基準の位置に影響する既知の方法のいずれかで、隣接点を調整してコンテンツ劣化させて、原信号を復元できるようにする。この検出基準には、いくつかの点どうしの関係を含めることができ、あるいは検出基準をしきい値交差と同様に単純にすることができ、あるいは検出基準にM個おきの点を含めることができる。隣接点の調整は、しきい値交差後の点にNを乗算することと同じくらい簡単にすることができる。Nが１未満であるが０に等しくなく、このため飽和及びデータ点が０に等しくなることが問題にはならず、そしてしきい値が正であり、しきい値交差中にデータが０に向かって減少することが有利である。

【０２２０】

このプロセスは、データ全体を通して検出基準を探索し、そして隣接点を元の値に再調整することを含むことができる。例えば、劣化プロセスにおける調整がNの乗算を用いる場合には、復元プロセスでは1/Nを乗算する。

【０２２１】

次の説明では、ディジタルコンテンツとは、オーディオ、ビデオ、及び画像を含む、知覚される物理的アイテム（事項）を表現するディジタルデータのことで

ある。ディジタルデータとは、一瞬時における元のディジタルコンテンツのサンプルを表現するビット（１または０）をグループ化したものである。各ビットグループは、データ点またはサンプルと等価なものを称する。データ点は、多くの場合にデータ列対時間または周波数を表現する順序で配列される。これに加えて、ＭＰＥＧ標準圧縮のディジタルオーディオ及びビデオにおける場合のように、データ点を再グループ化して、おそらくはデータ列対周波数対時間を表現するために用いられるサブグループを形成することができる。ディジタルデータが、始点及び終点を伴う順序を有して、データの探索が可能であり、そして隣接点を相互に近接した点として規定できることが最も重要である。最後に、点とは、１つまたはいくつかの点のことを称する。

【０２２２】

図３６に劣化及び復元プロセスの概要を示し、図３７に、装置によって実現される、これらのプロセスに対応する手続きを示す。

【０２２３】

ディジタルコンテンツを劣化させるために（ボックス１００）、サンプル中で検出基準を探索する（ボックス２００、２１０、及び２２０）。バッファ内の最終データ点を検査した後に探索を停止して、利用可能ならば新たなバッファを提供する。現在技術の状況では既知であるように、バッファ間でデータ値を保存し合って、始点を適切に探索できるように最初のバッファを適切に初期化しなければならない。

【０２２４】

検出基準を見出すと、隣接点を調整してコンテンツに劣化が生じるようにする（ボックス２３０）。これらの点の調整により、検出基準の位置が変化しないか、あるいは既知の方法で変化するようにすべきであり、そうしなければ、データを元の値に再調整（復元）するための正しい位置の検出が容易ではなくなる。これに加えて、調整により飽和が生じるか、あるいは値が０になることを防ぐことが望ましい、というのは、元のデータ点が容易に復元可能ではなくなるからである。

【０２２５】

元のデータコンテンツを復元するために（ボックス１１０）、劣化させたデータ上で、劣化プロセスによって規定した検出基準を探索する（ボックス２００、２１０、及び２２０）。劣化プロセスが既知の方法で検出基準を変化させている場合には、ボックス２２０の復元用の検出基準は、劣化で用いたものとは異なる。基準の位置を見出すと、劣化プロセスで用いた方法の逆によって隣接データ点を再調整する（ボックス２３０）。

【０２２６】

このプロセスの例を図３８及び図３９に示す。この場合には（ボックス３００及び３１０）、検出基準は、データが０に向かう間の、正のしきい値（thr>0）でのしきい値交差（Ｃ言語の表記法を用いると：x[n-1]>thr && x[n]<thr、「&&」は「かつ」の意味）である（ボックス４００、４１０、及び４２０）。隣接点は、しきい値交差の後の点のみを含む（ボックス４３０）。データを劣化させるために、調整は、しきい値交差の後のデータ点（x[n]）にＮを乗算することを含み、ここでＮは１未満である（ボックス４３０）。このデータ点の値を低減することによって、検出基準の位置が変化しない。これに加えて、Ｎが（０に等しくはならないが）０に近くなるほど、より多くのディジタルコンテンツが劣化する。元のディジタルデータを復元するために、しきい値交差の後の点（x[n]）に1/Ｎを乗算する（ボックス４３０）。

【０２２７】

使用しうる単純な検出基準がさらに存在する。例えばデータ点をＭ個おきに劣化させることができる。この場合には、復元のための同期は、正しく劣化された位置を見出すまで、Ｍ個の点にわたってデータを操作することを必要としうる。これに加えて、ピーク値を用いて、ピーク後の点の値を低減することができる。これにより、復元プロセス用の検出基準が影響されないことが望ましい。あるいはまた、負のしきい値でのしきい値交差、及び０に向けたデータ移動が実行可能である。ここでも、しきい値交差後のデータ点の絶対値を０に向けて低減するが、０に等しくはしない。後の２つの場合については、データを探索する際に、復元のための同期が発生する。

【０２２８】

元のディジタルデータの劣化と復元とで検出基準が変化しないことが好ましいが、これは要求ではない。既知の方法であれば、検出基準を変化させて、復元プロセスが、劣化プロセスとは異なる（既知の）検出基準を用いるようにする。換言すれば、劣化及び復元プロセスについて、ボックス４２０（上述のように、または２２０）が異なってくる。

【０２２９】

既に仮定しているかもしれないが、元のコンテンツは、ディジタルサンプル対時間によって表現する必要がない。ＭＰＥＧ圧縮を用いる場合（即ちＭＰ３オーディオ）のように多くの場合には、ディジタルサンプルが周波数対時間のサブグループを表現する。この場合には、サブグループ毎に周波数にわたってデータを探索するか、あるいは周波数毎に時間にわたってデータを探索するか、あるいは十分良く規定した他の組合わせにおいてデータを探索する。このデータは、周波数の大きさまたはこれに対応するスケールファクタのいずれかを表現することもできる。

【０２３０】

これに加えて、知覚上の劣化の大部分を除去しつつデータを復元する代わりの方法が存在する。例えば、低域通過フィルタを用いてデータを復元することができる。復元したディジタルデータは元のディジタルデータと正確には一致しないが、知覚上は許容できるものである。ＤＳＰの現在技術の状況に精通した者には周知のように、フィルタの種類及び次数のようなフィルタ特性が、復元したデータに影響する。

【０２３１】

あるいはまた、擬似ランダム列（キーとも別称される）を用いて、検出基準（ボックス２２０）あるいはデータの調整及び再調整（ボックス２２０）を設定するかことができる。このランダム性により、データの違法な復元に対する困難性が増加する。例えば、０より大きく１未満の擬似乱数を、スケール値として用いることができる（ボックス４３０）。あるいは、最小及び最大しきい値間の擬似乱数を、しきい値に用いることができる。劣化及び復元プロセスが同じ擬似ランダム列を用いるということがすべてである。しかし、この構成はデータと共にキ

ーを送ることを必要とする。既知の技法を用いて、キーをデータ内に埋め込んで、劣化したデータから原データをまだ復元できるようにする。

【０２３２】

図４０に、上述した劣化及び復元プロセスを実現するために使用するハードウエアを示す。このハードウエアは、論理プロセッサ５００及び記憶装置５１０を含む。論理プロセッサ５００は、ディジタル信号プロセッサ（ＤＳＰ）、汎用中央処理装置（ＣＰＵ）、メディアプロセッサを含むがこれに限定されない特化したＣＰＵと同等のものとして規定することができる。適切なＤＳＰチップは、テキサスインスツルメンツ社のTMS320製品ラインナップのうちの１つである。ＣＰＵは、インテル社のPentium(登録商標)ラインナップまたはモトローラ/ＩＢＭ社のPowerPC製品ラインナップを含むことができる。論理プロセッサ５００の制御用のコードの設計は、以上の擬似符号についての記述が与えられれば、現在技術の状況に精通した者にとっては簡単である。ディジタルプロセッサを用いる際には、記憶装置５１０がＲＡＭを含み、現在のバッファ及び／または検出基準に対して前の点を記憶する必要がある。

【０２３３】

これに加えて、現在技術の状況に精通した者は、論理プロセッサ５００を、アナログ及びディジタル回路で、独立回路または特定用途向け集積回路（ＡＳＩＣ）のいずれかの形で実現することができる。これらのアナログ及びディジタル回路は、次のデバイスのあらゆる組み合わせを含むことができる：ディジタルーアナログ変換器（D/A）、比較器、サンプルーホールド回路、遅延素子、アナログーディジタル変換器（A/D）、及びプログラマブルロジックコントローラ（ＰＬＣ）。

【０２３４】

スクランブル技術を改良する他の方法によれば、ヘッダまたはコンテンツについての他の重要な情報のスクランブルを回避するステップをプロセスに設ける。ヘッダをそのままにしておくことの利点は、アプリケーションまたは装置が、スクランブル解除及びコンテンツへのアクセス前に、コンテンツについての情報を即座に読み込めるということである。例えば、スクランブルしたＭＰ３ファイル

では、ユーザが歌を選択してスクランブル解除して演奏する前に、歌の長さ、演奏者、分解能、等について即座に知ることができる。あるいはまた、ヘッダに著作権情報を含めることができ、プレーヤは再生前にこの情報をチェックすることを要求される。

【０２３５】

スクランブルプロセスは、ヘッダ以外のコンテンツの一部または全部をスクランブルする。ヘッダ以外のコンテンツの一部のみをスクランブルした場合には、エラー訂正があっても、エラー訂正ではまず修復しきれないものとなる。コンテンツがフレームを含み、その各々が各自のヘッダを有する場合には、ＭＰＥＧ（Motion Pictures Expert Group）圧縮のオーディオまたはビデオで行ったように、各フレームのヘッダを回避しつつ、ヘッダ以外のコンテンツの一部または全部をスクランブルする。スクランブル解除プロセスは、スクランブルしたコンテンツから元のコンテンツを復元し、同様にヘッダ情報を回避する。

【０２３６】

好適なプロセスは、擬似ランダムノイズ（ＰＮ）列及びＸＯＲ関数を用いて、各フレームのヘッダを回避しつつコンテンツをスクランブルすることを含む。ＸＯＲ関数の逆もＸＯＲ関数であるので、スクランブル解除器はスクランブル器と同一とすることができる。

【０２３７】

ここでも、用語の吟味を順番に行う。ファイルのヘッダは、ファイルについての重要な情報を含んでいる。この情報は、ファイルの種類、作成者、作成場所、作成日、最終変更日、ファイルのサイズ、構造、アロケーション（割り当て）、著作権コード、固有のＩＤ、ユーザ規則、等を含むことができる。ヘッダはファイルの先頭のみ、フレームの先頭のみ、あるいはこれらの両方に存在しうる。ＭＰＥＧオーディオ及びビデオのような圧縮したディジタルメディアにとっては、フレームは通常のものである。より詳細には、ＭＰ３データでは、ＭＰＥＧの標準ラベルがヘッダとするもの、エラー訂正、及びサイド情報をヘッダに含めることができる。これに加えて、コンテンツがフレームまたはヘッダを含まない場合には、こうしたデータを新たに構築したファイルフォーマットで容易に作成する

ことができる。

【０２３８】

図３３に、スクランブルプロセスの概要を示す。ファイルが、グローバルヘッダのみか、あるいは同期符号（sync）なしの既知のサイズのフレームを有する場合には、スクランブルステップ中には（ボックス１１０）ヘッダの位置を特定してこれを飛ばす（ボックス１０５）。換言すれば、同期符号を探索する理由が存在しない（ボックス１００）。スクランブルのステップでは、ヘッダ以外のコンテンツの一部または全部をスクランブルすることができる。追加的な同期符号を有するフレームにファイルを分割している場合には、フレームを規定する同期符号を見出して（ボックス１００）、ヘッダ情報を飛ばして（ボックス１０５）コンテンツをスクランブルする（ボックス１１０）。通常、ヘッダはフレームのサイズについての情報を含み、これは次の同期符号の位置を特定することの助けとなる、というのは、同期符号もデータ内でランダムに発生するからである。ここでも、スクランブルのステップで、ヘッダ以外のコンテンツの一部または全部をスクランブルすることができる。

【０２３９】

スクランブルのステップは、従来法で用いている方法で構成することができる。ＤＥＳまたはＲＳＡのような、標準的な近代の暗号化が最良の選択である。この暗号化では、１つのファイルは力ずくでスクランブル解除できるが、同じキーを用いても、他のファイルは安全なままにしておくことができる。他のスクランブルの選択肢は、ＰＮ列を伴う、乗算、加算、減算または排他的論理和（ＸＯＲ）のような単純な数学的演算を含むことができる。限られたビット長分割の不正確な特性によるビットエラーが発生しうるので、分割は慎重に用いるべきである。

【０２４０】

図３３に、スクランブル解除プロセスの概要を示す。スクランブル解除はスクランブルの逆であり、スクランブルしたコンテンツのビットのみをスクランブル解除すべきである。ファイルが、グローバルヘッダのみか、あるいは同期符号（sync）のない既知のサイズのフレームを有する場合には、ヘッダの位置を特定し

て、スクランブル解除のプロセス中に（ボックス１６０）これを飛ばす（ボックス１５５）。換言すれば、同期符号を探索すべき理由が存在しない（ボックス１５０）。ファイルが同期符号を有するフレームに分割されている場合には、フレームを規定する同期符号を見出して（ボックス１５０）、ヘッダ情報を飛ばして（ボックス１５５）、当該フレーム内の残りのコンテンツをスクランブル解除する（ボックス１６０）。通常、ヘッダはフレームのサイズについての情報を含み、これは同期符号の位置を特定することの助けとなる、というのは、同期符号は独特のものではなく、このためデータの中に発生するからである。スクランブル解除のステップは、ヘッダ以外のコンテンツの一部または全部をスクランブル解除することができる。

【０２４１】

スクランブル解除器は、スクランブル器が用いる関数の逆の関数を用いるべきものである。標準的な近代の暗号化でするランブルした際には、スクランブル解除器は暗号解読キーを必要とし、このキーは暗号キーとは異なるものとすることができる。数学的演算については、減算と加算は互いに逆であり、ＸＯＲの逆もＸＯＲであり、除算は乗算の逆である。スクランブル解除では除算が使用可である、というのは、スクランブルのプロセスにおける乗算器がスクランブル解除では除算器になるため、余りがないことは既にわかっているからである。

【０２４２】

スクランブルとスクランブル解除の両方で、多くのフレームについて、そしておそらくはコンテンツのトラック全体についても、キーが同じままであると想定され、このトラックは歌または映画で構成することができる。このため放送では、おそらくはトラック毎にキーが変化し、キーを送る方法が多数存在することは、暗号化法の現在技術の状況に精通した者にとって明らかである。ＰＮ列を用いる際には、以下に記述するように、ＰＮ列用のキーはＰＮ列の発生関数であり、このキーはＭＰ３の歌毎に変化せず、即ちトラックとして規定される。なお、この発生関数は毎回同一のランダム列を作成し、このことは暗号化法の現在技術の状況では周知である。あるいはまた、歌のようなあらゆるコンテンツのトラックは、限られた全体（グローバル）リストからの１つ以上のキーを用いることがで

きる。

【０２４３】

図３４ａに、スクランブル及びスクランブル解除のプロセスの一例用の擬似符号を示す。この例では、コンテンツが同期符号で始まるフレームを含み、フレーム毎にヘッダが存在する。ＸＯＲの逆関数もＸＯＲそのものであるので、スクランブル及びスクランブル解除のプロセス用の擬似符号は同一とすることができる。

【０２４４】

この簡単な例によってスクランブル及びスクランブル解除したコンテンツは、階層III（ＭＰ３）またはＡＡＣのようなＭＰＥＧオーディオデータを含むことができる。ＭＰＥＧオーディオの同期符号は「1111 1111 1111」である。こうした方法には多くの利点がある。例えば、ユーザが歌を再生することを決心する前に、携帯プレーヤが、歌の長さ、演奏者、分解能、等についての情報を即座に表示することができる。同様に、ヘッダが著作権情報を含むことができ、プレーヤが再生を行う前に、この情報をチェックすることを要求される。

【０２４５】

このプロセスは、コンテンツの先頭から始まる（ボックス２００）。次に同期符号を見出し、これは通常コンテンツの最初の２、３ビットにある（ボックス２０５）。次にヘッダデータを飛ばし、これはできれば、同期符号の後のデータからヘッダのサイズ分を読み込んで行う（ボックス２１０）。次に、コンテンツのＭビットとＰＮ列のＭビットとのＸＯＲ演算を用いて、当該フレームのコンテンツのＭビットをスクランブルする（ボックス２１５）。図３４ｂに、ＸＯＲ関数についての入力及び出力を示す。次にコンテンツをチェックして、他のフレームが存在するか否かを見極める（ボックス２２０）。他のフレームが存在する場合には、ボックス２０５からプロセスを継続し、ここでは同期符号の位置を特定する。通常、フレームのサイズはフレームのヘッダから読み取ることができ、これは次の同期符号を探索する助けとなる。コンテンツが残っていない場合には、プロセスを完了する（ボックス２２５）。

【０２４６】

この例では、Ｍの大きさにより、強力な攻撃に対する強固さが決まり、ここでは攻撃者の目的は、元のコンテンツを入手することである。Ｍが大きいほど、スクランブルしたコンテンツがより強固になる。しかしＭが小さいほど、スクランブル及びスクランブル解除のプロセスがより効率的になりうる。Ｍは、エラー訂正によって修復可能なビット数より大きく、かつ当該フレームのヘッダ以外のコンテンツのビット数よりも小さい任意の数とすることができる。

【０２４７】

フレーム内でスクランブルしたＭビットの位置が既知であり、かつこのＭビットがコンテンツの完全性にとって重要なビットを含んでいなければならない。これらのビットはヘッダの後のＭビットとすることができる。しかし、ＭＰ３データでは、フレームのデータがヘッダの後から始まらなくても構わない。この場合には、スクランブルするビットは当該フレームのデータの最初のＭビットとすることができる。これらのビットによりオーディオビットの割り当て（アロケーション）が決まり、これらのビットはファイルの完全性にとって重要なものである。

【０２４８】

図３５に、スクランブル及びスクランブル解除のプロセス用に適したハードウエアを示す。このハードウエアは、ディジタル論理プロセッサ３００とディジタルメモリ３１０を含む。この論理プロセッサは、このプロセスの算術計算及び論理演算を実行する。論理プロセッサ３００は、ディジタル信号プロセッサ（ＤＳＰ）、汎用中央処理装置（ＣＰＵ）、メディアプロセッサまたは特定用途向け回路（ＡＳＩＣ）を含めた特化したＣＰＵと同等のものとすることができる。適切なＤＳＰチップはテキサスインスツルメンツ社のTMS320製品ラインナップのうちの１つである。ＣＰＵは、インテル社のPentium(登録商標)ラインナップまたはモトローラ/ＩＢＭ社のPowerPC製品ラインナップのうちの１つを含むことができる。ＡＳＩＣは、現在技術の状況に精通した人が、以上の擬似符号及び記述により容易に設計することができる。制御用の論理プロセッサ３００の設計も、現在技術の状況に精通した人にとっては、以上の擬似符号及び記述が与えられれば簡単である。ディジタルプロセッサを使用する際には、メモリ３１０がＲＡＭを含

み、メモリ３１０はプログラム及び他に必要な変数を記憶するために用いる。

【０２４９】

（結び）

以上、種々の実施例を参照しながら本発明の原理について説明してきたが、こうした原理を逸脱することなく、本発明の基本構成及び詳細を変更しうることは明らかである。

【０２５０】

例えば、多くの実施例は透かし技術を採用して対称物またはコンテンツを識別しているが、これは本質的なことではない。適切な環境であれば、他のマーキング（標識付け）技法を採用することもできる。

【０２５１】

同様に、あるプロセスについては、ユーザに対して所定の位置で実行するものとして説明してきたが、こうしたプロセスの位置は一般に重要ではない。即ち、（安全性の問題を適切に応えていれば）現在状況にとって最も有益であるように、タスクを処理装置間に割り振ることができる。

【０２５２】

本明細書では画像及びビデオを含めた応用を参照しながら説明しており、好適なオーディオ応用に焦点を置いたのでは、こうしたことがあいまいになる。従って、上述した技法は、オーディオ以外の他の形態のメディアにも同等に適用可能であることを特に強調しておく。

【０２５３】

単一のサンプル値系を変化させる実施例について詳細に説明してきたが、他の実施例では、例えば改ざんが存在すれば透かしの耐性を増加させることのように、隣接する複数のサンプル値系を変化させることが望ましい。

【０２５４】

同様に、補助データをコンテンツに埋め込む実施例について詳細に説明してきたが、補助データの表現形態については詳細には説明していない。一部の実施例では、Ｎビットのペイロード（実質的なデータ）をＭビットに符号化し、ここでＭ＞Ｎである（即ち、部分的または全体的な冗長性を有する）。この冗長性は、

コンテンツ全体中でのＮビットペイロードの反復、このＮビットの、ＢＣＨ－符号化、慣例の符号化、ターボ符号化、その他の符号化を行って、強固さ及び／またはエラー訂正、即ちＣＲＣ符号またはＥＣＣ符号を提供することを含みうる。

【０２５５】

以上詳述した実施例は多くの部分から成るシステムであるが、その個別の構成要素にも新規性が存在すること、及びこれらの構成要素は他のシステム及び装置にも採用可能であることは明らかである。

【０２５６】

以上に詳述した実施例における要素及び特徴の特定の組合わせは好適なものに過ぎず、これらの教示を他のものと交換及び代替すること、及び参考文献に記載の教示と交換及び代替することも考えられる。

【０２５７】

以上説明した原理及び特徴を適用しうる広範な種々の実施例から見れば、詳述した技術は例示的なものであり、本発明の範囲を限定するものではないことは明らかである。請求項に記載のこと及びこれと同等のことの範囲から考案されるすべての変形例も本発明に含まれる。

【図面の簡単な説明】

【図１】　埋め込み技法で用いる動作を示すフローチャートである。

【図２】　図１の方法を用いてデータを埋め込みまたは復帰するために使用する装置を示すブロック図である。

【図３】　復号化技法で用いる動作を示すフローチャートである。

【図４】　第１実施例の動作を図式的に示す図である。

【図５】　第１実施例によるデータの埋め込みを示すフローチャートであり、破線は補助データとのやり取りを示す。

【図６】　データの復号化を示すフローチャートであり、破線は補助データとのやり取りを示す。

【図７】　第２実施例の動作を図式的に示す図である。

【図８】　第２実施例によるデータの埋め込みを示すフローチャートであり、破線は補助データとのやり取りを示す。

【図９】　データの復号化を示すフローチャートであり、破線は補助データとのやり取りを示す。

【図１０】　実施例の要点を、ディジタル圧縮技法と関連付けて示す図である。

【図１１】　図１１Ａ及び図１１Ｂは、実施例による埋め込み及び復帰装置を示すブロック図である。

【図１２】　データ埋め込み用の、図２の装置の具体例を示す図である。

【図１３】　データ復帰用の、図２の装置の具体例を示す図である。

【図１４】　攻撃対抗に関する説明で参照したプロセスを可能にするブロック図である。

【図１５】　登録プロセスを示すフローチャートである。

【図１６】　動的ロックにより補助データの複製をブロックする方法を示す図である。

【図１７】　排他的論理和（ＸＯＲ）関数用の入力及び出力を示す図である。

【図１８】　図１８Ａは、動的ロック及び補助データの埋め込みのプロセスの概要を示す図であり、図１８Ｂは、補助データの復帰及びロック解除のプロセスの概要を示す図である。

【図１９】　図１９Ａは、局所的にマスクした埋め込みデータ用の動的ロックの修正ステップを示す図であり、図１９Ｂは、パルス幅変調（ＰＷＭ）した埋め込みデータ用の動的ロックの修正ステップを示す図であり、図１９Ｃは、ＰＮシーケンスにもとづく実施例用の動的ロックの修正ステップを示す図である。

【図２０】　図２０Ａは、ヘッダブロックを用いて、補助データをロックして埋め込む手続きを、フローチャートの形式で示す図であり、図２０Ｂは、ヘッダブロックを用いて、補助データをロック解除して復帰する手続きを、フローチャートの形式で示す図である。

【図２１】　利用例の背後にある基本プロセスを示す図である。（破線のボックスは随意的なものである。破線で囲んだボックス郡は同様のアイテムを表わす。これに加えて、３つのキー位置を示してあるが、通常は１つのキーのみを使用し、その位置は利用法での要求に依存する。最後に、略称ＩＤを用い、多くの場合には識別子を称するが、何らかの補助的情報を称することもある。）

【図２２】　強固なデータ埋め込み技法に使用できる装置を示す図である。

【図２３】　動的ロック用の図２２の装置の具体例を示す図である。

【図２４】　動的ロック解除用の図２２の装置の具体例を示すブロック図である

【図２５】　自動ＩＤ管理のプロセスの概要を示す図である。

【図２６】　好適な自動ＩＤ管理プロセスを実現するための擬似符号を示す図である。

【図２７】　自動ＩＤ管理を実現する装置を示す図である。

【図２８】　図２７の装置を含む携帯ＭＰ３オーディオプレーヤを示す図である。

【図２９】　２つの透かしを用いるプロセスの概要を示す図である。

【図３０】　図２９の埋め込みプロセス用の擬似符号を示す図である。

【図３１】　図２９の復帰プロセス用の擬似符号を示す図である。

【図３２】　図２９のプロセスに関連して使用しうる装置を示す図である。

【図３３】　図３３ａは、スクランブルプロセスの概要を示す図であり、点線のボックスはオプションであり、図３３ｂは、スクランブル解除プロセスの概要を示す図であり、点線のボックスはオプションであ。

【図３４】　図３４ａは、好適なスクランブル及びスクランブル解除プロセス用の擬似符号を示す図であり、図３４ｂは、排他的論理和（ＸＯＲ）関数用の入力及び出力を示す図である。

【図３５】　スクランブル及びスクランブル解除プロセスの実行用の好適な装置を示す図である。

【図３６】　劣化及び復元プロセスを示す図である。

【図３７】　図３６の劣化及び復元プロセス用の擬似符号を示す図である。

【図３８】　しきい値交差及び次の点のみの調整を用いた劣化及び復元プロセスの、単純かつ効率的な例を示す図である。

【図３９】　図３６の劣化及び復元プロセス用の擬似符号を示す図である。

【図４０】　図３６～図３９のプロセスを実現するのに適した装置の概要を示す図である。

【図１】

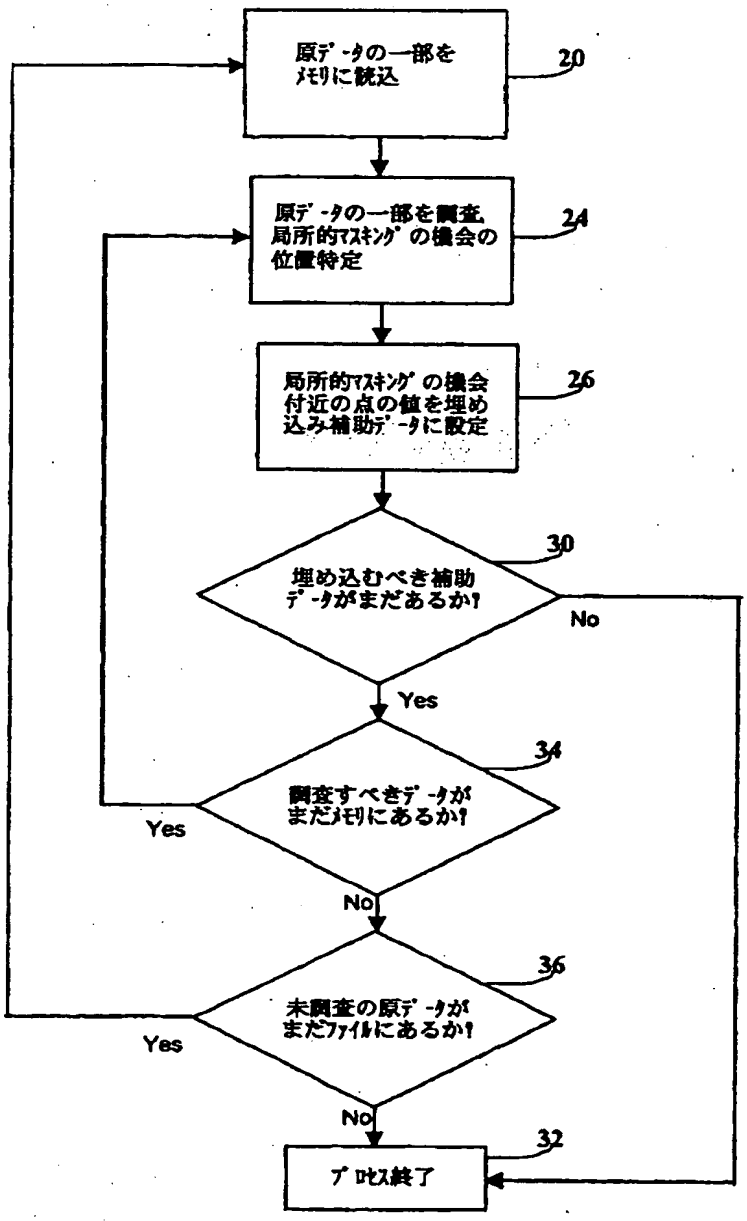


Fig 1

【図２】

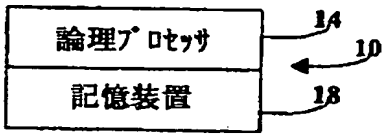


Fig. 2

【図３】

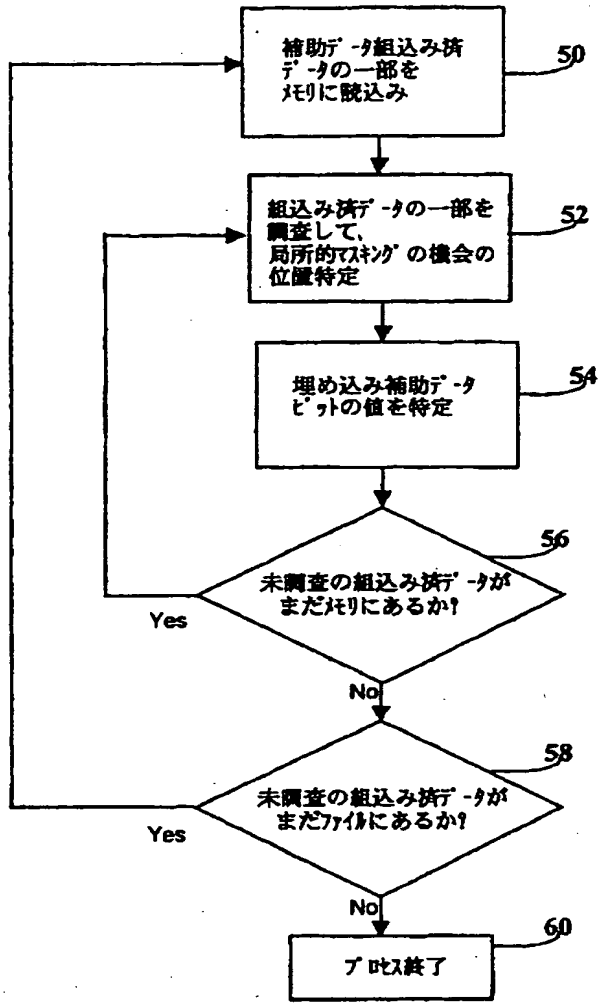


Fig 3

【図４】

Fig. 4

【図５】

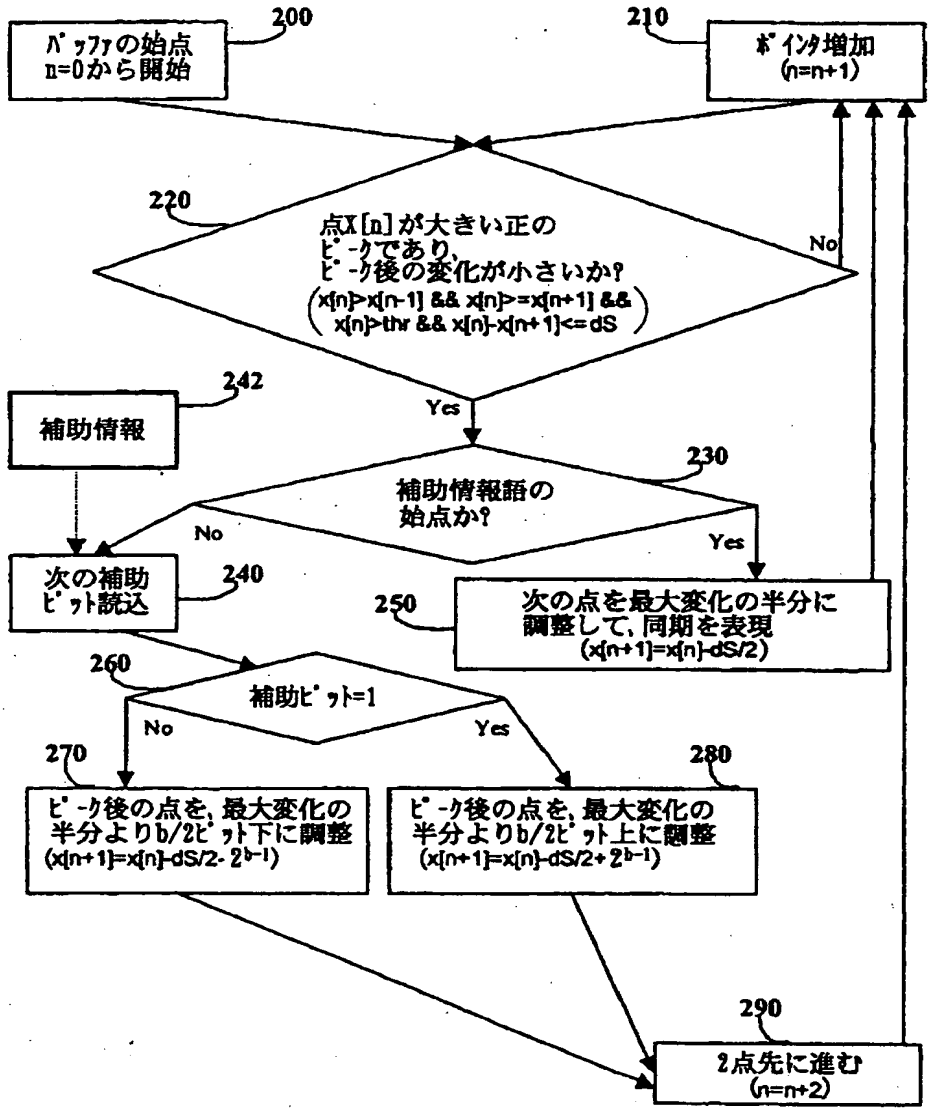

バッファの始点
n=0から開始
200
ポインタ増加
(n=n+1)
210
220
点X[n]が大きい正の
ピークであり,
ピーク後の変化が小さいか?
(x[n]>x[n-1] && x[n]>=x[n+1] &&
x[n]>thr && x[n]-x[n+1]<=dS
No
Yes
242
補助情報
230
補助情報語の
始点か?
No
Yes
次の補助
ビット読込
240
250
次の点を最大変化の半分に
調整して, 同期を表現
(x[n+1]=x[n]-dS/2)
260
補助ビット=1
No
Yes
270
280
ピーク後の点を, 最大変化の
半分よりb/2ビット下に調整
(x[n+1]=x[n]-dS/2-2^(b-1))
ピーク後の点を, 最大変化の
半分よりb/2ビット上に調整
(x[n+1]=x[n]-dS/2+2^(b-1))
290
2点先に進む
(n=n+2)

Fig. 5

【図６】

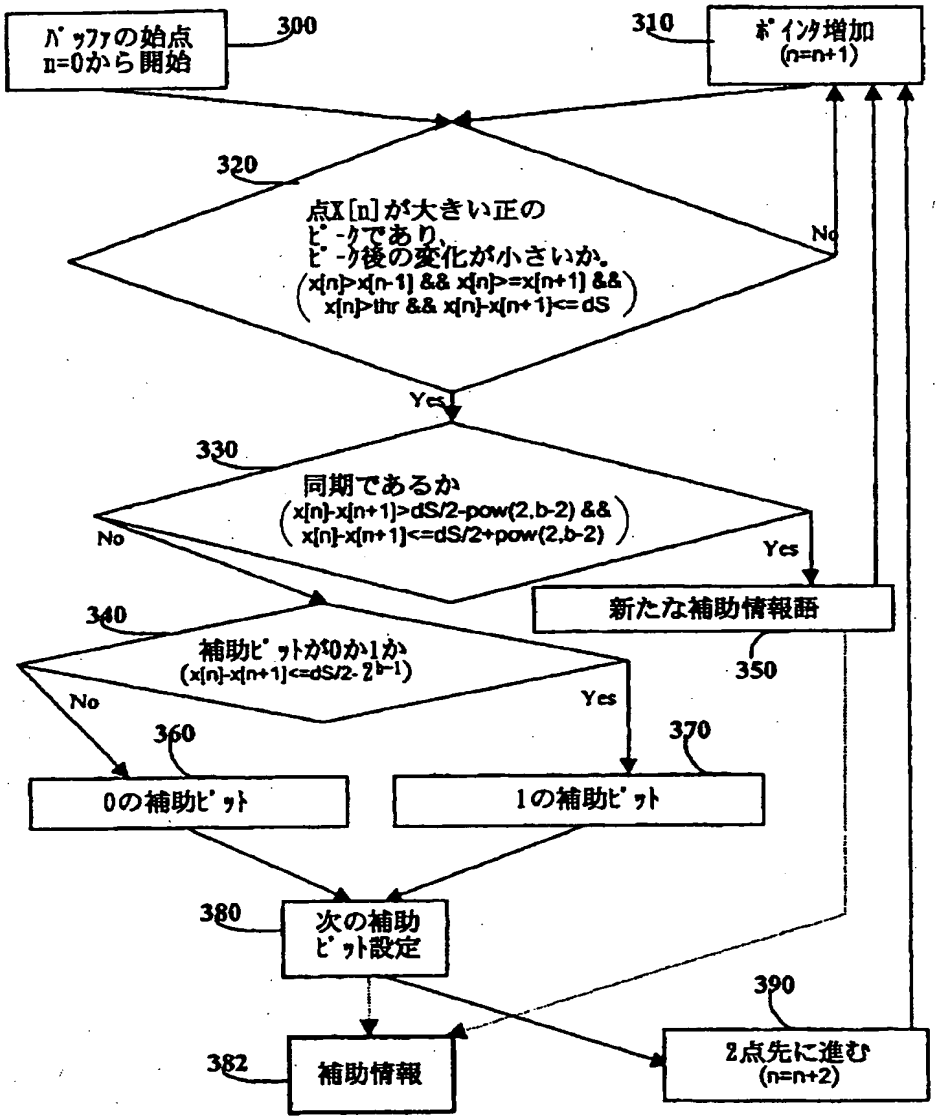


Fig. 6

【図７】

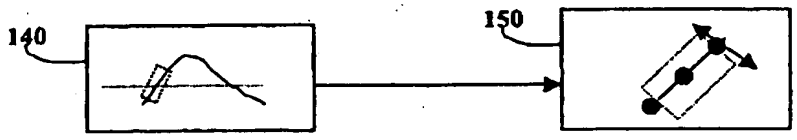


Fig. 7

【図８】

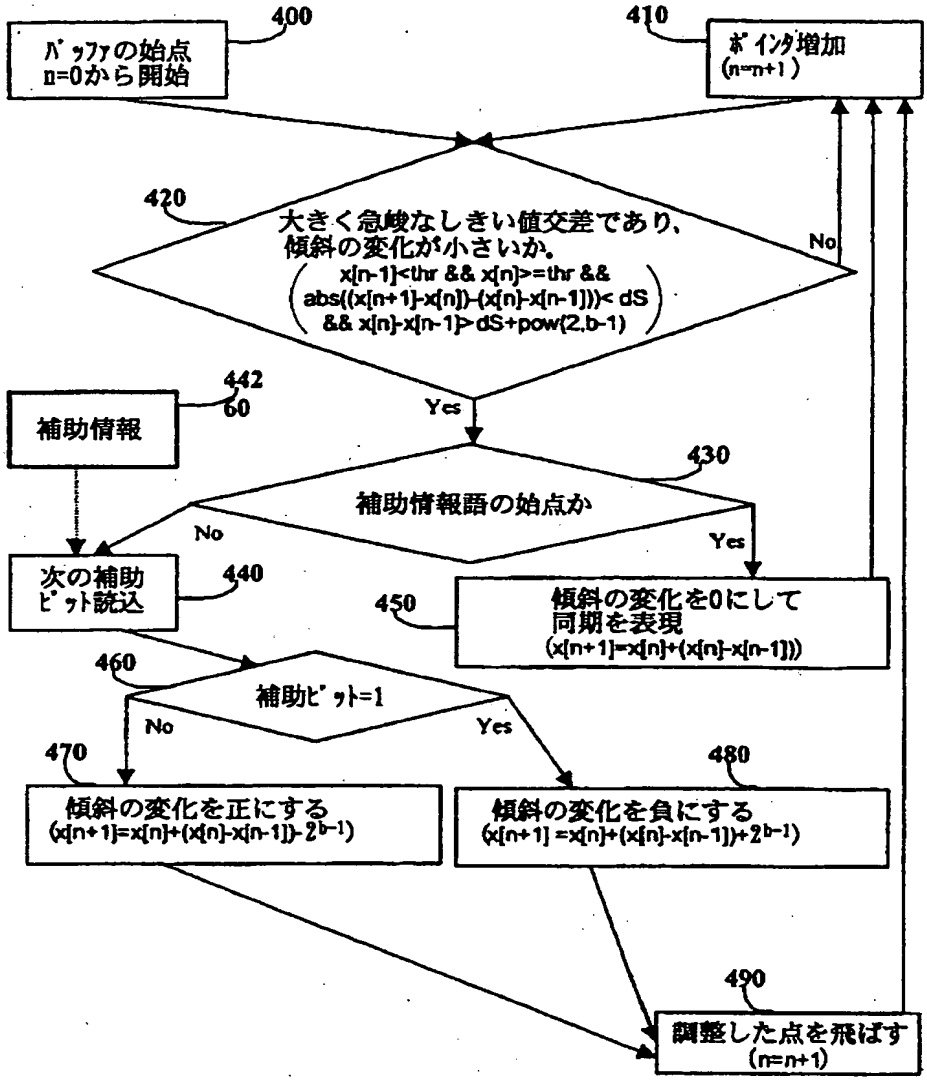

400
バッファの始点
n=0から開始
410
ポインタ増加
(n=n+1)
420
大きく急峻なしきい値交差であり、
傾斜の変化が小さいか。
x[n-1]<thr && x[n]>=thr &&
abs((x[n+1]-x[n])-(x[n]-x[n-1]))< dS
&& x[n]-x[n-1]>dS+pow(2,b-1)
No
Yes
442
60
補助情報
430
補助情報語の始点か
No
Yes
次の補助
ビット読込
440
450
傾斜の変化を0にして
同期を表現
(x[n+1]=x[n]+(x[n]-x[n-1]))
460
補助ビット=1
No
Yes
470
傾斜の変化を正にする
(x[n+1]=x[n]+(x[n]-x[n-1])-2^(b-1))
480
傾斜の変化を負にする
(x[n+1] =x[n]+(x[n]-x[n-1])+2^(b-1))
490
調整した点を飛ばす
(n=n+1)

Fig. 8

【図９】

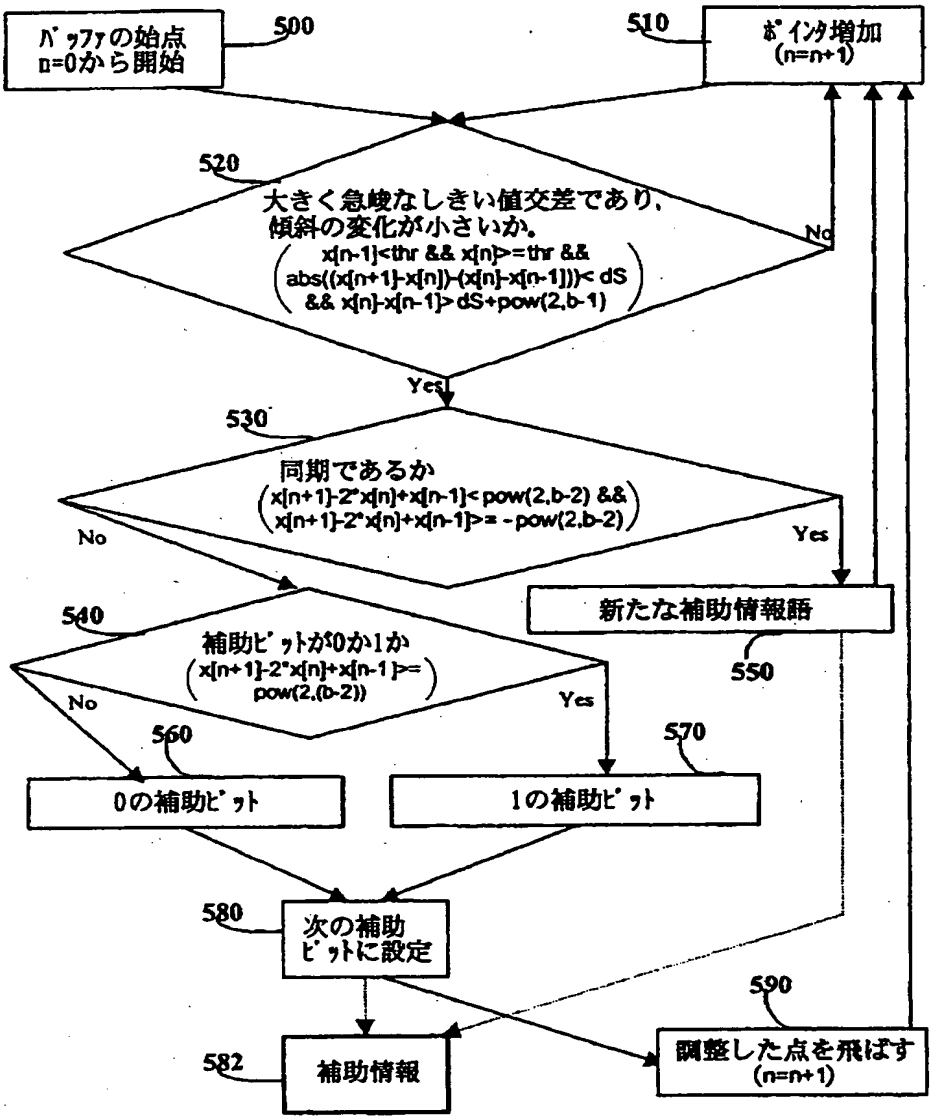

バッファの始点
n=0から開始
500
510
ポインタ増加
(n=n+1)
520
大きく急峻なしきい値交差であり、
傾斜の変化が小さいか。
x[n-1]<thr && x[n]>=thr &&
abs((x[n+1]-x[n])-(x[n]-x[n-1]))< dS
&& x[n]-x[n-1]> dS+pow(2,b-1)
No
Yes
530
同期であるか
x[n+1]-2*x[n]+x[n-1]< pow(2,b-2) &&
x[n+1]-2*x[n]+x[n-1]>= -pow(2,b-2)
No
Yes
新たな補助情報語
550
540
補助ビットが0か1か
x[n+1]-2*x[n]+x[n-1]>=
pow(2,(b-2))
No
Yes
560
570
0の補助ビット
1の補助ビット
580
次の補助
ビットに設定
590
582
補助情報
調整した点を飛ばす
(n=n+1)

Fig. 9

【図１０】

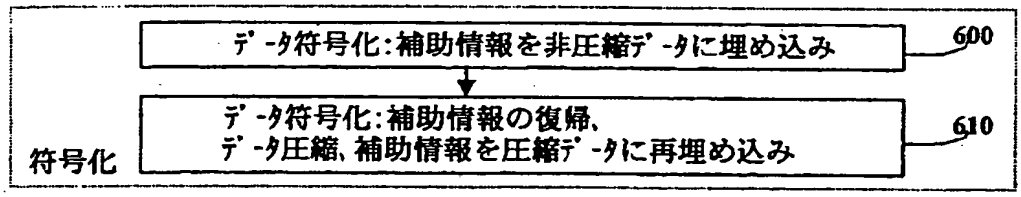


Fig. 10A

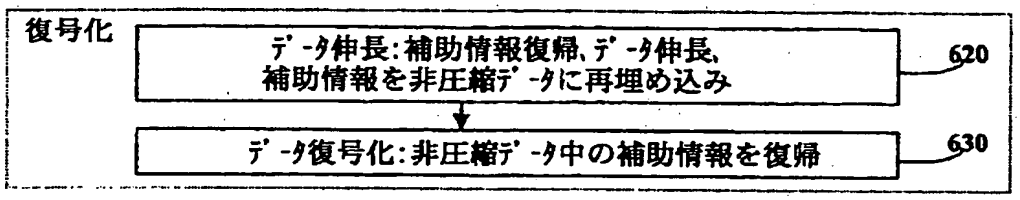


Fig. 10B

【図１１】

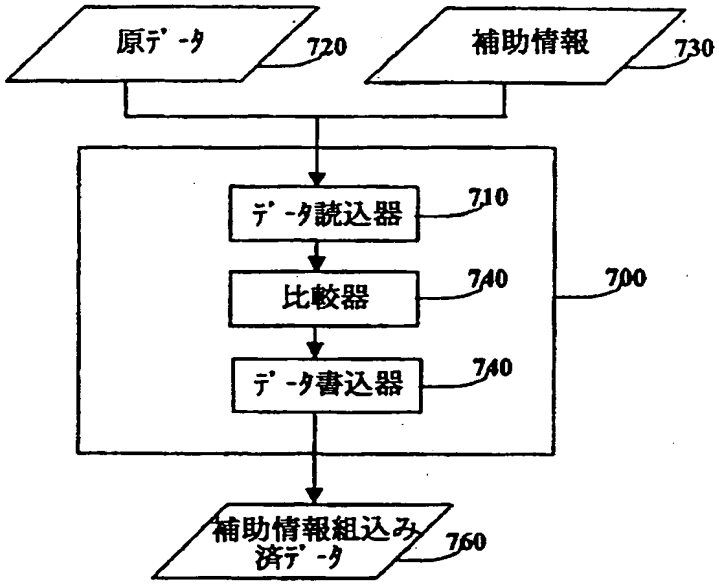


Fig. 11A

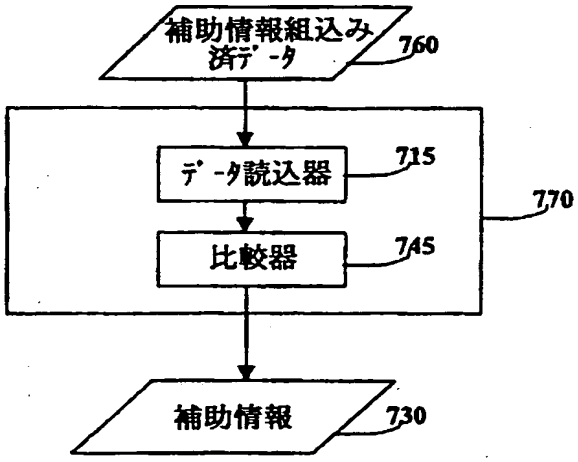


Fig. 11B

【図１２】

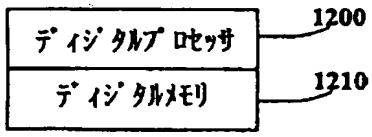


Fig. 12

【図１３】

A/D変換器	ｻﾝﾌﾟﾙ/ﾎｰﾙﾄﾞ	D/A変換器
比較器	PLC	遅延

Fig 13

【図１４】

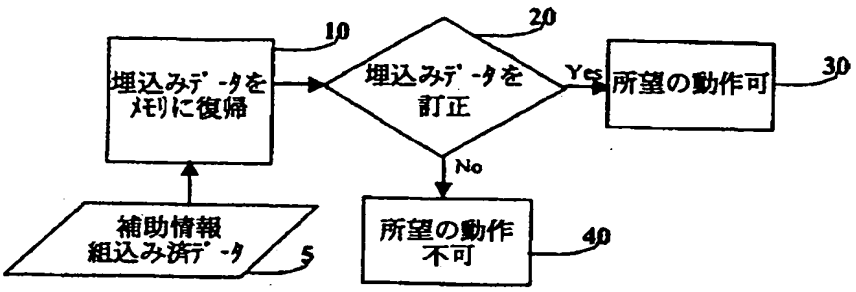


Fig. 14

【図１５】

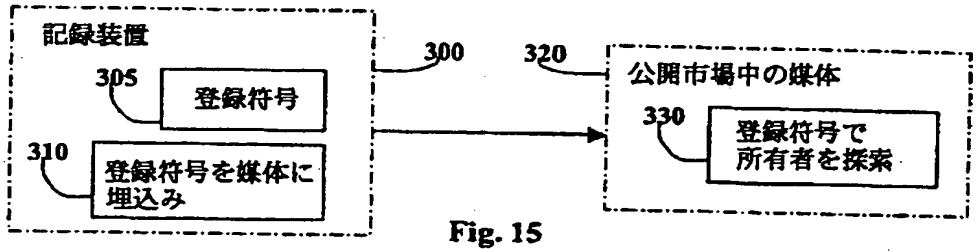


Fig. 15

【図１６】

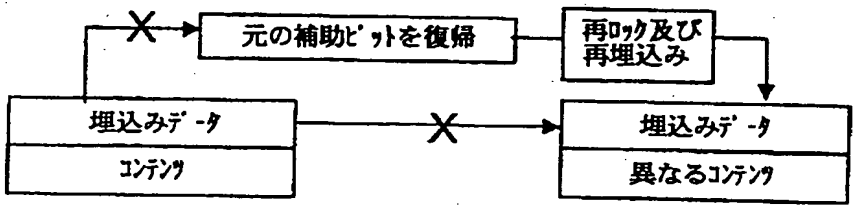


Fig. 16

【図１７】

XOR

d	c	f(d,c)
1	1	0
1	0	1
0	1	1
0	0	0

Fig. 17

【図１８】

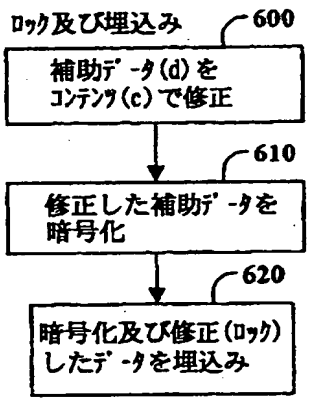


Fig. 18A

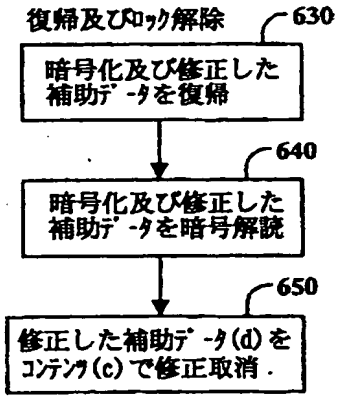


Fig. 18B

【図１９】

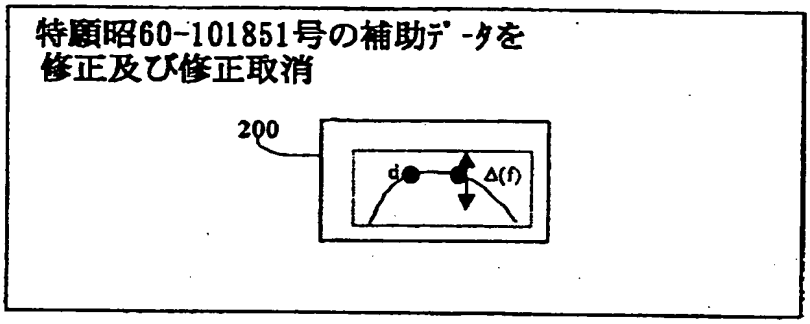


Fig. 19A

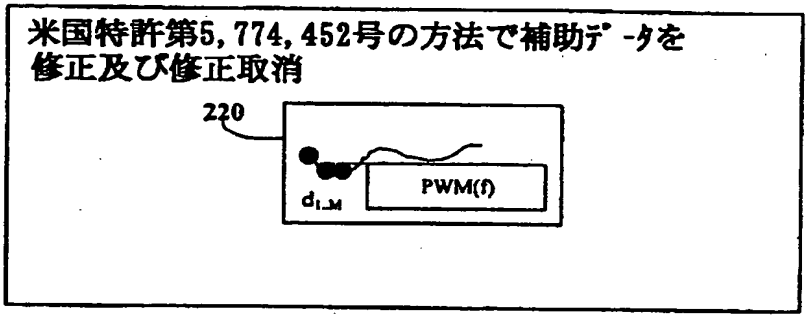


Fig. 19B

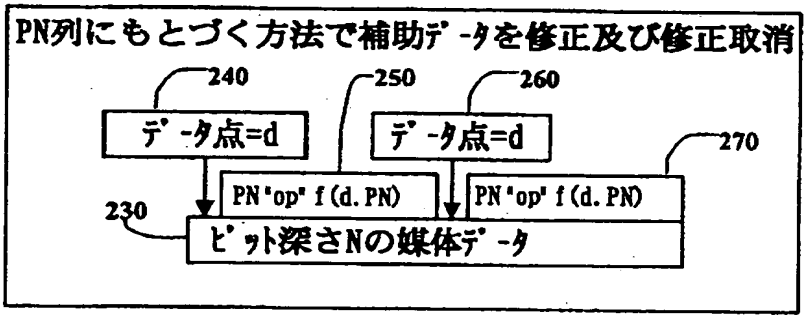


Fig. 19C

【図２０】

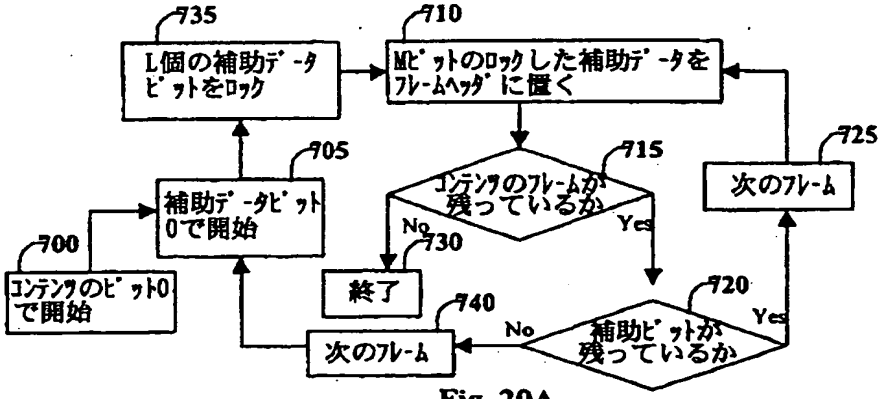


Fig. 20A

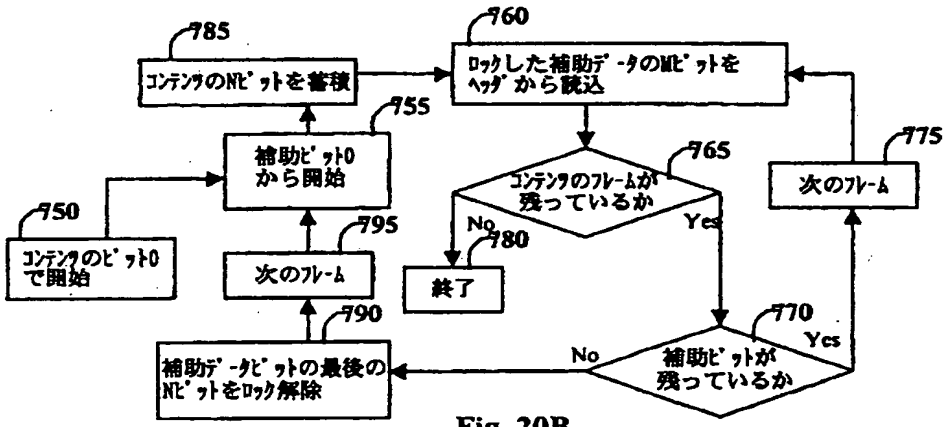


Fig. 20B

【図２１】

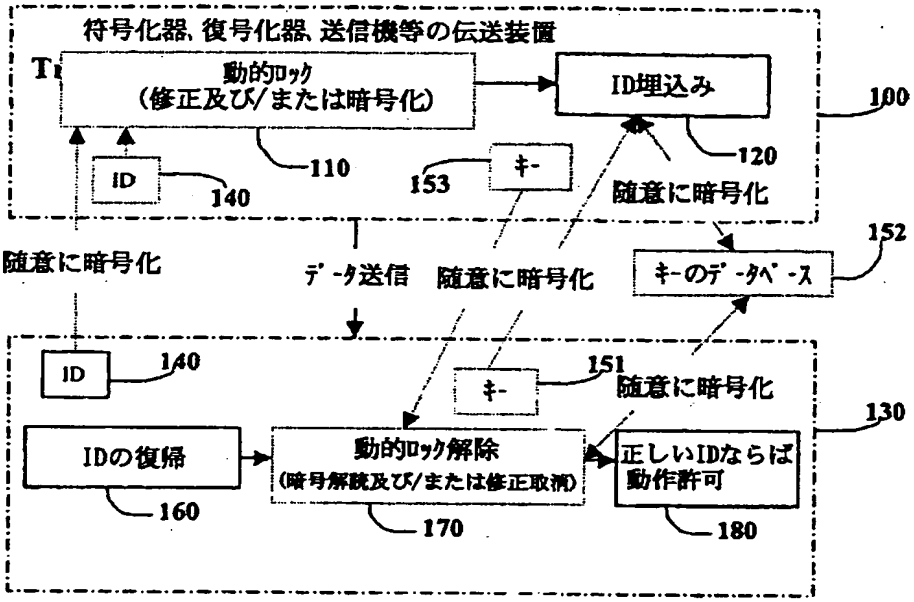


Fig. 21

【図２２】

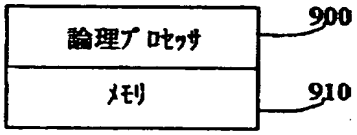


Fig. 22

【図２３】

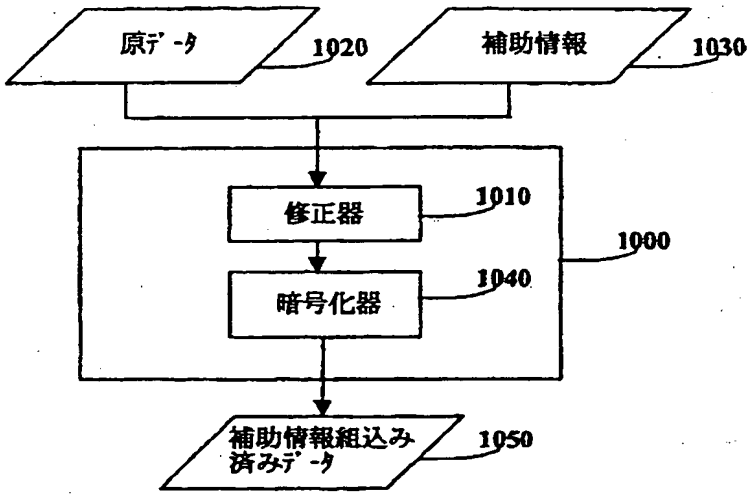


Fig. 23A

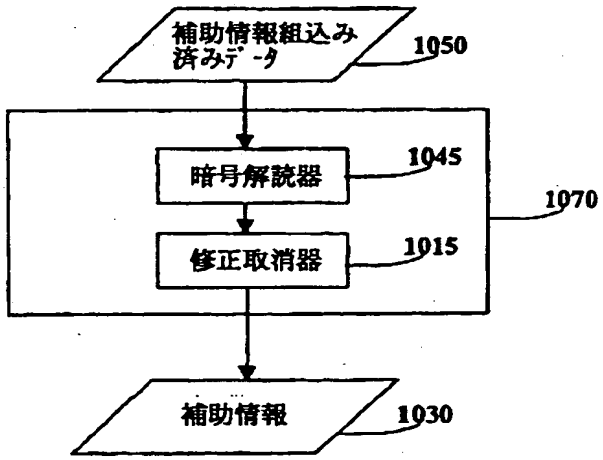


Fig. 23B

【図２５】

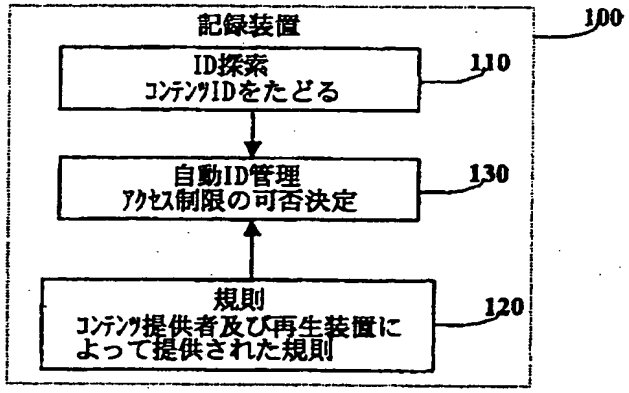


Fig. 25

【図２６】

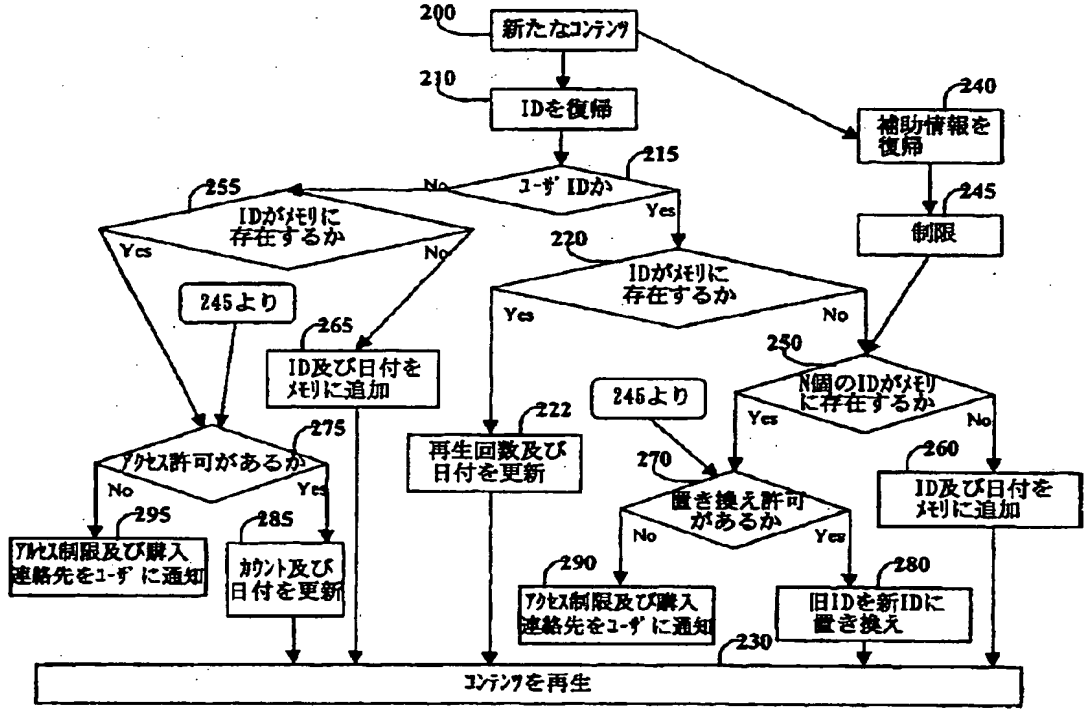


Fig. 26

【図２７】

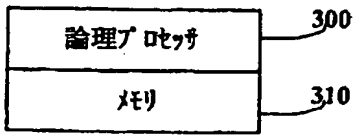


Fig. 27

【図２８】

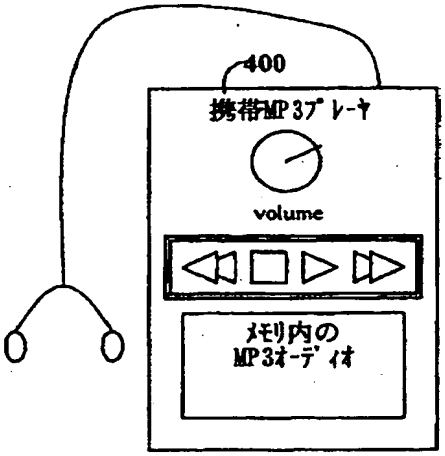


Fig 28

【図２９】

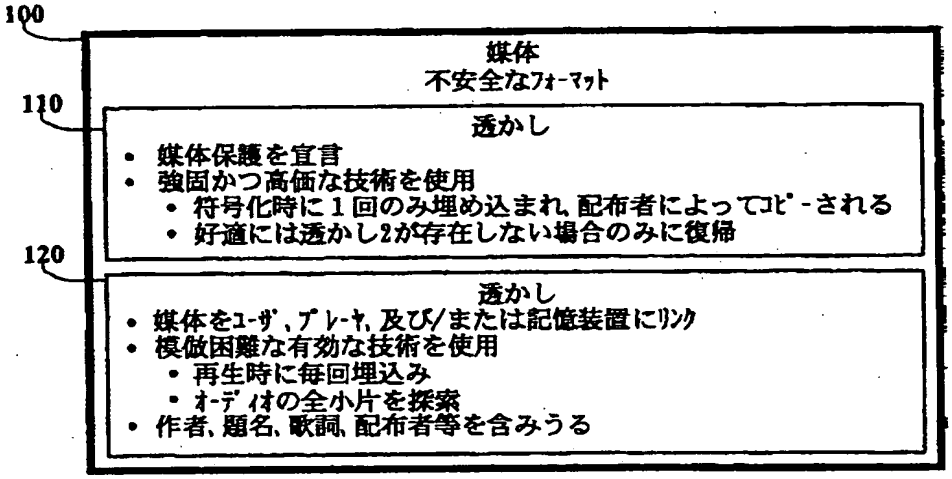


Fig. 29

【図３０】

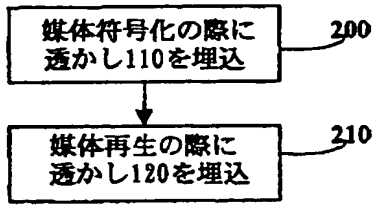


Fig. 30

【図３１】

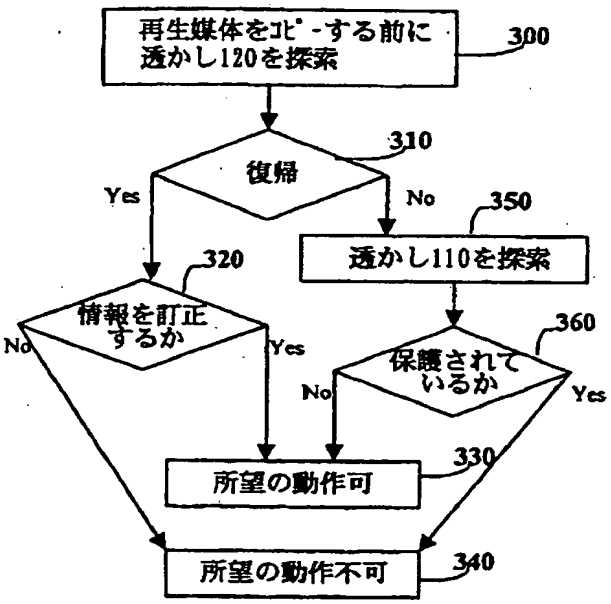


Fig. 31

【図３２】

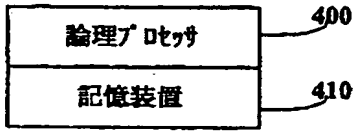


Fig. 32

【図３３】

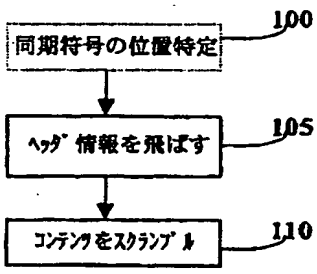


Fig. 33a

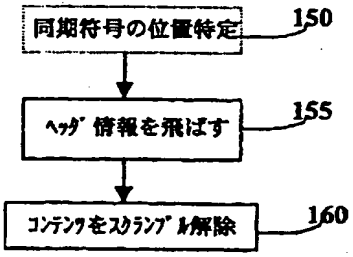


Fig. 33b

【図３４】

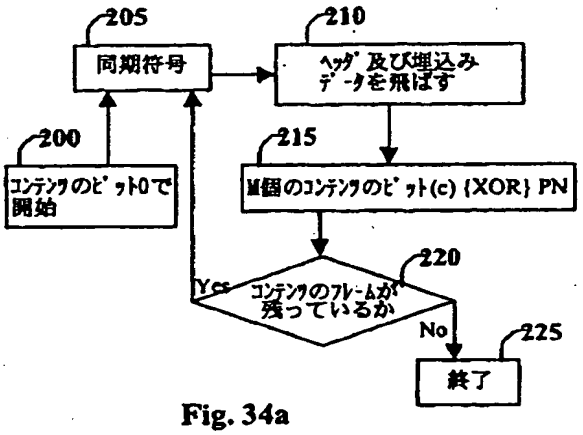


Fig. 34a

XOR

c	PN	f(c,PN)
1	1	0
1	0	1
0	1	1
0	0	0

Fig. 34b

【図３５】

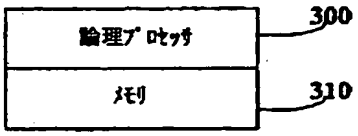


Fig. 35

【図３６】

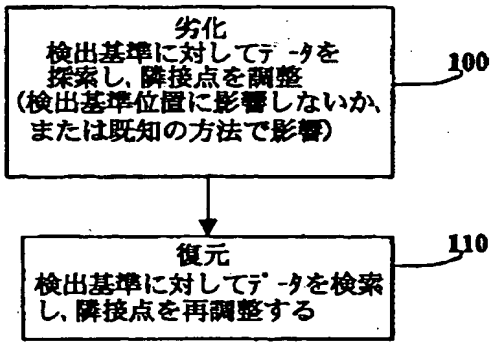


Fig. 36

【図３７】

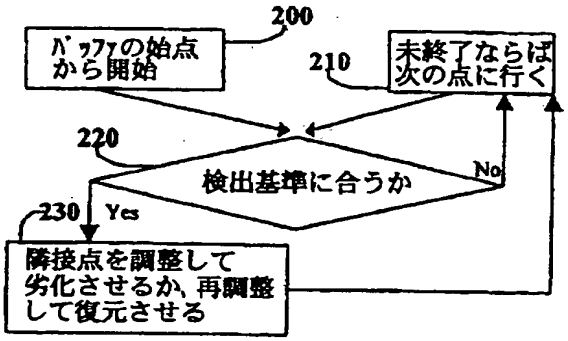


Fig. 37

【図３８】

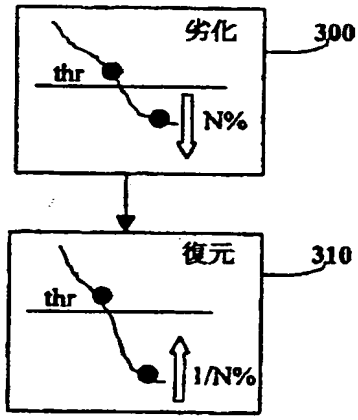


Fig. 38

【図３９】

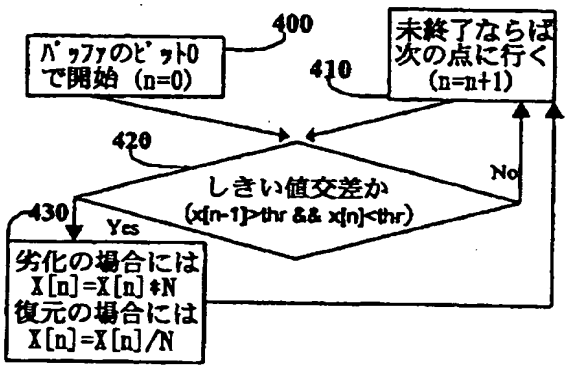


Fig. 39

【図４０】

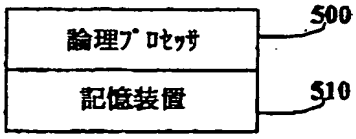


Fig. 40

【手続補正書】

【提出日】平成１３年１０月１日（２００１．１０．１）

【手続補正１】

【補正対象書類名】図面

【補正対象項目名】図２３

【補正方法】変更

【補正の内容】

【図２３】

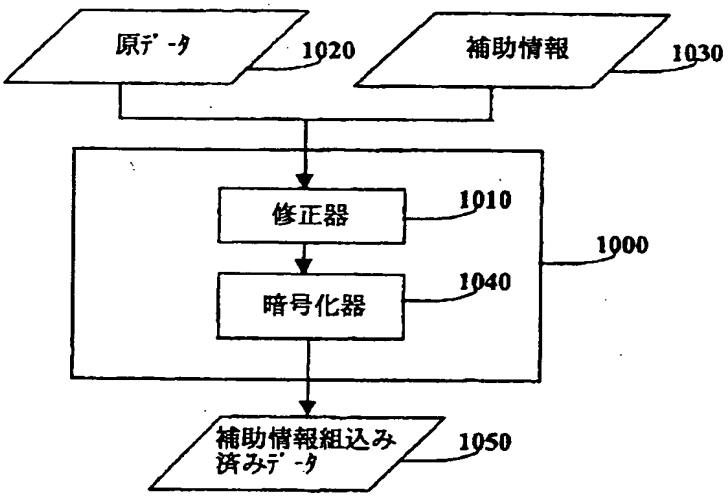


Fig. 23

【手続補正２】

【補正対象書類名】図面

【補正対象項目名】図２４

【補正方法】変更

【補正の内容】

【図２４】

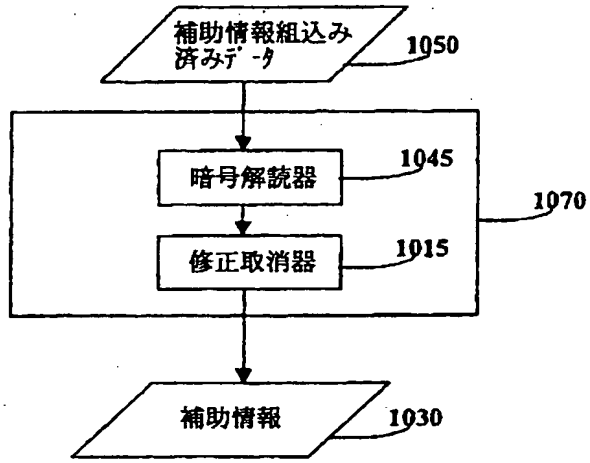


Fig. 24

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inter..ational application No.
PCT/US00/06296

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) : H04L 9/00
US CL : 713/168, 176
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/168, 176

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
East, West

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P — Y, P	US 6,021,196 A (SANDFORD, II et al) 01 February 2000 (01.02.2000), abstract, columns 2-3, lines 62-33.	1-3, 8-9 — 7
X — Y	US 5,721,788 A (POWELL et al) 24 February 1998 (24.02.1998), abstract, figures 2A, 2, 3, and 5, column 4, lines 13-39.	1-6, 8-9 — 7
Y, P	US 5,930,369 A (COX et al) 27 July 1999 (27.08.1999), abstract, column 7, lines 16-37.	7
A, E	US 6,061,793 A (TEWFIK et al) 09 May 2000 (09.05.2000), ALL.	1-9
A, E	US 6,049,627 A (BECKER et al) 11 April 2000 (11.04.2000), ALL.	1-9
A, E	US 6,044,182 A (DALY et al) 28 MARCH 2000 (28.03.2000), ALL.	1-9
A, P	US 5,943,422 A (VAN WIE et al) 24 AUGUST 1999 (24.08.1999), ALL.	1-9
A, P	US 5,912,972 A (BARTON) 15 JUNE 1999 (15.06.1999), ALL.	1-9
A	US 5,875,249 A (MINTZER et al) 23 FEBRUARY 1999 (23.02.1999), ALL.	1-9

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 May 2000 (30.05.2000)	05 JUL 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Tod Swann For Eugenia Logan Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	ﾃｰﾏｺｰﾄﾞ(参考)
H04N 7/08		H04N 7/08	Z
7/081			

(31)優先権主張番号　６０／１２６，５９１
(32)優先日　平成11年３月26日(1999. 3. 26)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　６０／１２６，５９２
(32)優先日　平成11年３月26日(1999. 3. 26)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／４０４，２９２
(32)優先日　平成11年９月23日(1999. 9. 23)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／４０４，２９１
(32)優先日　平成11年９月23日(1999. 9. 23)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＧＷ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＧＭ，ＫＥ，ＬＳ，ＭＷ，ＳＤ，ＳＬ，ＳＺ，ＴＺ，ＵＧ，ＺＷ)，ＥＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＥ，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＡ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＵ，ＣＺ，ＤＥ，ＤＫ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＤ，ＧＥ，ＧＨ，ＧＭ，ＨＲ，ＨＵ，ＩＤ，ＩＬ，ＩＮ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＣ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＳＬ，ＴＪ，ＴＭ，ＴＲ，ＴＴ，ＵＡ，ＵＧ，ＵＳ，ＵＺ，ＶＮ，ＹＵ，ＺＡ，ＺＷ

(72)発明者　ケネス　エル　レヴィ
アメリカ合衆国　ワシントン州　98648
スティーヴンソン　エヌイー　セダール
ストリート　110

Ｆターム(参考)　5B057 BA01 CE08 CG07
5C063 AB03 AB05 AC01 AC05 DA13
5C076 AA14 BA06
5J104 AA14

【要約の続き】
ヘッダからの情報）をスクランブルしないまま自由にアクセス可能とするような方法で、コンテンツをスクランブルして有利にしている。